

Criptografia: les matemàtiques de la informació secreta

Xevi Guitart

Departament de Matemàtiques i Informàtica
Universitat de Barcelona

Breu introducció històrica

- **Criptografia ve del grec krypto (amagar) i grapho (escriure).**
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com "el xifrat del Cèsar"
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a "trencar" el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com "el xifrat del Cèsar"
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a "trencar" el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com “el xifrat del Cèsar”
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a “trencar” el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com “el xifrat del Cèsar”
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a “trencar” el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com “el xifrat del Cèsar”
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a “trencar” el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com “el xifrat del Cèsar”
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a “trencar” el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Criptografia ve del grec krypto (amagar) i grapho (escriure).
- L'objectiu és transmetre missatges de manera privada, que només siguin comprensibles pels destinataris autoritzats i per ningú més
- Durant molt de temps, pràcticament els únics usuaris d'aquestes tècniques eren els militars i els governs.
 - ▶ Els grecs ja feien servir tècniques de xifrat (segle III aC)
 - ▶ Juli Cèsar (~ 45 aC) feia servir un mètode que avui en dia es coneix com “el xifrat del Cèsar”
 - ▶ Al-Kindi, un matemàtic àrab (segle VII d.C.) fou el primer a “trencar” el xifrat del Cèsar.
 - ▶ Va jugar un paper molt important en la segona guerra mundial (màquina Enigma).

Breu introducció històrica

- Als anys 70 del segle passat hi ha una revolució en la criptografia:

Breu introducció històrica

- Als anys 70 del segle passat hi ha una revolució en la criptografia:
 - ▶ Ús creixent de la informàtica i les comunicacions digitals:
 - ★ demanda de serveis criptogràfics per part de la societat civil
 - ★ entitats financeres i empreses en general

Breu introducció històrica

- Als anys 70 del segle passat hi ha una revolució en la criptografia:
 - ▶ Ús creixent de la informàtica i les comunicacions digitals:
 - ★ demanda de serveis criptogràfics per part de la societat civil
 - ★ entitats financeres i empreses en general
 - ▶ 1976: invenció de la criptografia de **clau pública** per Whitfield Diffie i Martin Hellman, matemàtic i enginyer electrònic americans.



Breu introducció històrica

- Als anys 70 del segle passat hi ha una revolució en la criptografia:
 - ▶ Ús creixent de la informàtica i les comunicacions digitals:
 - ★ demanda de serveis criptogràfics per part de la societat civil
 - ★ entitats financeres i empreses en general
 - ▶ 1976: invenció de la criptografia de **clau pública** per Whitfield Diffie i Martin Hellman, matemàtic i enginyer electrònic americans.



- ▶ 1978: Rivest, Shamir i Adelman inventen el criptosistema **RSA**
 - ★ Àmpliament utilitzat avui en dia a internet

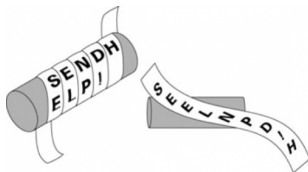


Alguns xifrats històrics: l'escítal

- Utilitzat pels espartants $\sim$ 400 a.C.

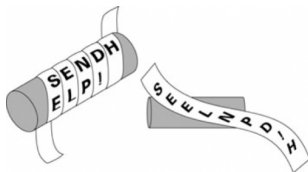
Alguns xifrats històrics: l'escítal

- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



Alguns xifrats històrics: l'escítal

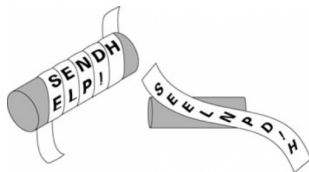
- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



- Quan desenrotllem el paper, les lletres queden desordenades (es fa una permutació) i no s'entén el missatge

Alguns xifrats històrics: l'escítal

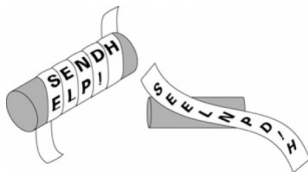
- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



- Quan desenrotllem el paper, les lletres queden desordenades (es fa una permutació) i no s'entén el missatge
- Per a desxifrar-lo, l'enrotllem en un bastó...

Alguns xifrats històrics: l'escítal

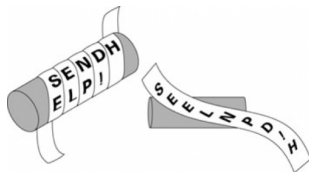
- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



- Quan desenrotllem el paper, les lletres queden desordenades (es fa una permutació) i no s'entén el missatge
- Per a desxifrar-lo, l'enrotllem en un bastó...del mateix diàmetre!

Alguns xifrats històrics: l'escítal

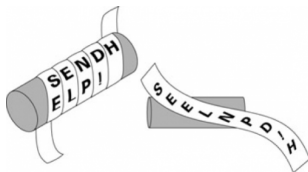
- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



- Quan desenrotllem el paper, les lletres queden desordenades (es fa una permutació) i no s'entén el missatge
- Per a desxifrar-lo, l'enrotllem en un bastó...del mateix diàmetre!
- Emissor i receptor han d'haver acordat el diàmetre, **la clau secreta**

Alguns xifrats històrics: l'escítal

- Utilitzat pels espartans ~ 400 a.C.
- Un bastó on s'hi enrotlla una tira de paper, i s'hi escriu el missatge



- Quan desenrotllem el paper, les lletres queden desordenades (es fa una permutació) i no s'entén el missatge
- Per a desxifrar-lo, l'enrotllem en un bastó...del mateix diàmetre!
- Emissor i receptor han d'haver acordat el diàmetre, **la clau secreta**
- És un xifrat de **permutació**

Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - És la mida de la graella, en aquest cas 3×5

Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - ▶ És la mida de la graella, en aquest cas 3×5

Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - ▶ És la mida de la graella, en aquest cas 3×5

Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - ▶ És la mida de la graella, en aquest cas 3×5

Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - ▶ És la mida de la graella, en aquest cas 3×5

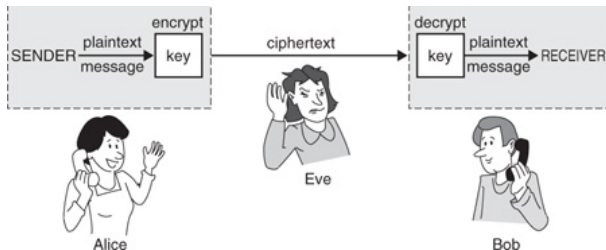
Un altre xifrat de permutació

- Missatge: Ataqueu a les vuit
- Omplim una graella per files

A	T	A	Q	U
E	U	A	L	E
S	V	U	I	T

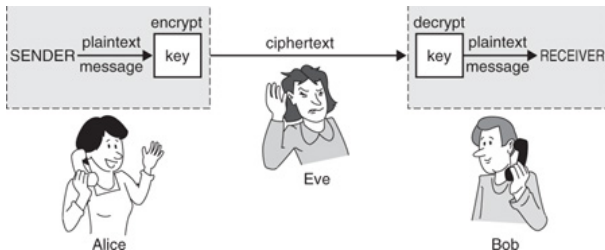
- Llegim per columnes: AESTUVA AUQLIUET
- Per dexifrar: omplim la graella per columnes i llegim per files
- Quina és ara la clau secreta?
 - ▶ És la mida de la graella, en aquest cas 3×5

El xifrat del Cèsar



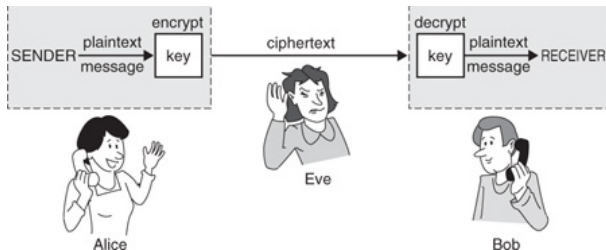
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de **substitució**

El xifrat del Cèsar



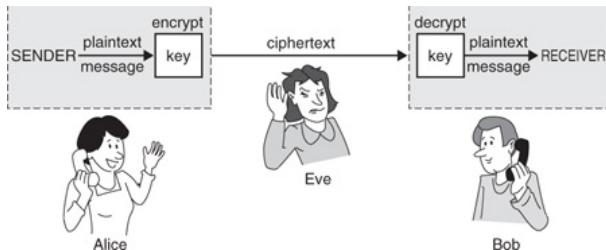
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de **substitució**

El xifrat del Cèsar



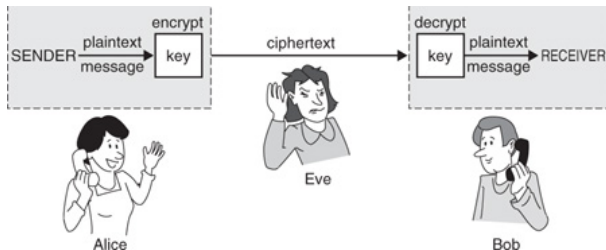
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de **substitució**

El xifrat del Cèsar



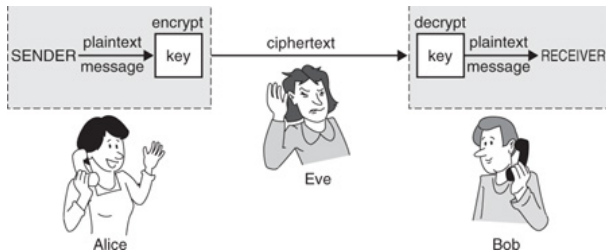
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de **substitució**

El xifrat del Cèsar



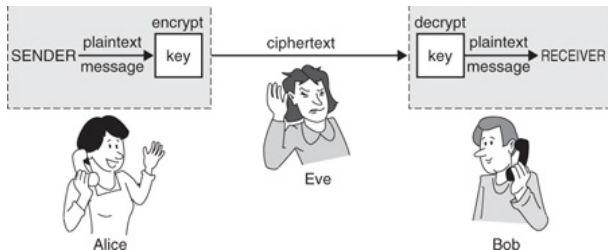
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de substitució

El xifrat del Cèsar



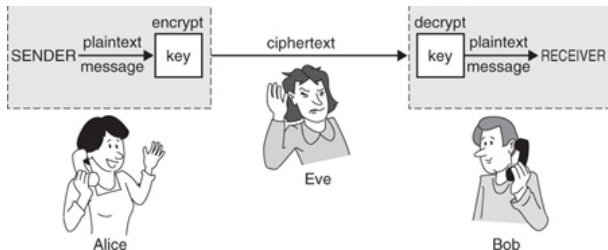
- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de substitució

El xifrat del Cèsar



- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de substitució

El xifrat del Cèsar



- L'Alice i en Bob es reuneixen prèviament i acorden substituir cada lletra per la que està 3 posicions més endavant a l'alfabet
- Així si el missatge és HOLA, l'Alice el xifra i transmet KROD.
- En Bob rep KROD, i per desxifrar-lo substitueix cada lletra per la que està 3 posicions més enrera a l'alfabet, obtenint HOLA.
- L'Eve intercepta KROD, i no sap el seu significat.
- La clau k és el nombre de posicions que tirem a la dreta.
- Diuen que aquest sistema, amb $k = 3$, era utilitzat per Juli Cèsar.
- Aquest és un xifrat de **substitució**

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Comptem! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Comptem! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Comptem! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Comptem! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Comptem! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ $7\ 14\ 11\ 0 \rightarrow 1\ 8\ 5\ 20$
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Comptem! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Comptem! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Comptem! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dóna ≥ 26 , hem de restar-li 26
 - ▶ $7\ 14\ 11\ 0 \rightarrow 1\ 8\ 5\ 20$
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dóna < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dóna ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dóna < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dóna ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dóna < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Xifrat de substitució i aritmètica modular

- L'alfabet català té 26 lletres, identifiquem lletres amb nombres:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- Podem identificar l'alfabet amb $\{0, 1, 2, \dots, 25\}$.
- Un missatge és una cadena de nombres: HOLA $\rightarrow$ 7 14 11 0
- L'Alice i en Bob acorden una clau secreta, per exemple $d = 20$
- Per xifrar sumem 20 al nombre associat a cada lletra
 - ▶ Compte! Si el resultat dona ≥ 26 , hem de restar-li 26
 - ▶ 7 14 11 0 $\rightarrow$ 1 8 5 20
 - ▶ HOLA $\rightarrow$ BIFU
- Per desxifrar, a cada lletra li hem de restar 20.
 - ▶ Compte! Si el resultat dona < 0 , aleshores li hem de sumar 26
- A aquesta manera de sumar i restar, en què volem portar els resultats a un nombre entre 0 i 25, se li diu **aritmètica mòdul 26**
- No és res nou per a nosaltres:
 - ▶ Quan sumem o restem hores ho fem mòdul 12
 - ▶ Quan sumem o restem angles, ho fem mòdul 360

Com podem trencar el xifrat del Cèsar?

- 1 Força bruta: hi ha 26 claus possibles, les podem provar totes...
- 2 Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la *E* = 4 s'ha xifrat com *R* = 17.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
 - ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
 - Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

Com podem trencar el xifrat del Cèsar?

- ❶ Força bruta: hi ha 26 claus possibles, les podem provar totes...
- ❷ Hi ha una manera millor, que és la que va descobrir Al-Kindi
 - ▶ Interceptem el missatge NGNDHRRH N YRF QRH QRY IRFCER
 - ▶ No totes les lletres són igual de freqüents
 - ▶ En català la més freqüent és la *E*.
 - ▶ En un text xifrat llarg, és probable que la lletra que aparegui més cops sigui la que es correspon a la *E*.
 - ▶ *R* apareix 6 cops, podem intuir que la $E = 4$ s'ha xifrat com $R = 17$.
 - ▶ Si desxifrem amb la clau $17 - 4 = 13 = N$ obtenim:
ATAQUEU A LES DEU DEL VESPRE
 - ▶ Altres pistes: Dígrafs habituals (RR, SS, QU, etc.)
- Aquests atacs es poden solucionar, amb els anomenats sistemes de substitució polialfabètica. Ara en veurem un exemple.
- Encara hi ha un problema: cal acordar una clau prèviament...

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - Però si sabem (o deduïm) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: “COSA”)
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: “COSA”)
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

El xifrat de Vigenere

- Com la substitució simple, però utilitzem més d'una clau
- Exemple: clau 2 14 18 0 (paraula clau: "COSA")
- Missatge: Ataqueu a les dotze

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17

- Missatge xifrat: chsqwsmanskdqhre
- Dificulta l'atac per força bruta: ara hi ha $26^n = 456\,976$ possibles claus, on n és la longitud de la clau.
- Dificulta l'anàlisi de freqüència: la primera A es xifra sumant 2, i la segona A es xifra sumant 18.
 - ▶ Però si sabem (o deduem) la longitud de la clau, podem fer anàlisi de freqüència per a cada posició
- Encara hi ha un problema: Cal acordar una clau prèviament.

Criptosistemes de clau secreta

Fenomen general

Com més llarga és la clau, més segur és el criptosistema.

Criptosistemes de clau secreta

Fenomen general

Com més llarga és la clau, més segur és el criptosistema.

- La màquina Enigma, o altres màquines de rotors, utilitzades durant la segona guerra mundial, eren dispositius mecànics que realitzaven substitució polialfabètica de període molt llarg.



Criptosistemes de clau secreta

- Avui en dia en comunicacions digitals
 - ▶ criptosistemes de clau secreta (combinen substitució i permutació)
 - ▶ AES: Advanced Encryption Standard (utilitzat a internet)

Criptosistemes de clau secreta

- Avui en dia en comunicacions digitals
 - ▶ criptosistemes de clau secreta (combinen substitució i permutació)
 - ▶ AES: Advanced Encryption Standard (utilitzat a internet)
- Com es fa per a compartir de manera segura la clau secreta?

Criptosistemes de clau secreta

- Avui en dia en comunicacions digitals
 - ▶ criptosistemes de clau secreta (combinen substitució i permutació)
 - ▶ AES: Advanced Encryption Standard (utilitzat a internet)
- Com es fa per a compartir de manera segura la clau secreta?
 - ▶ Aquí és on entren en joc els criptosistemes de **clau pública**, descoberts el 1976 per Diffie–Hellman.

Criptosistemes de clau secreta

- Avui en dia en comunicacions digitals
 - ▶ criptosistemes de clau secreta (combinen substitució i permutació)
 - ▶ AES: Advanced Encryption Standard (utilitzat a internet)
- Com es fa per a compartir de manera segura la clau secreta?
 - ▶ Aquí és on entren en joc els criptosistemes de **clau pública**, descoberts el 1976 per Diffie–Hellman.
 - ▶ Veurem el criptosistema RSA, el més utilitzat avui en dia



El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? *hi ha infinit!*
 - ▶ 12353245539999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA

- Idea: hi ha dues claus, una per a xifrar i l'altra per a desxifrar
 - ▶ La clau per a xifrar la sap tothom, és pública
 - ▶ La clau per a desxifrar, només la sap qui rep el missatge
- Treballem amb aritmètica modular, mòdul un nombre que sigui el producte de dos primers molt grans
 - ▶ un nombre és primer si només és divisible per 1 i per ell mateix
 - ▶ 2, 3, 5, 7, 11, 13, ... són primers, però 4, 6, 8, 9, 10, 12, ... no ho són
 - ▶ Quants nombres primers hi ha? N'hi ha infinits!
 - ▶ 1235324553999999981554151456773 és un primer de 30 xifres
- Per al sistema RSA cal:
 - ▶ Escollir dos primers molt grans: p i q
 - ▶ Calcular $N = p \cdot q$
 - ▶ Fer tots els càlculs amb aritmètica mòdul N
- Farem un exemple de joguina amb $p = 5$, $q = 11$, $N = 55$

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

El criptosistema RSA: un exemple de joguina

- Alice vol enviar un missatge a Bob. Aleshores Bob fa el següent:
 - ▶ Pren un producte de dos primers, per exemple $N = 5 \cdot 11 = 55$.
 - ▶ Fa públic el nombre 55, per ex. posant-lo a la seva web.
- L'Alice veu que la clau pública d'en Bob és $N = 55$.
 - ▶ Un missatge són nombres mòdul 55, és a dir nombres entre 0 i 54.
 - ▶ Suposem que el missatge és $m = 6$.
 - ▶ En comptes d'enviar m , enviem $m^3 \pmod{55}$. És a dir $6^3 = 216$, restant 55 tants cops com faci falta per fer-lo caure entre 0 i 54.
 - ▶ Resulta que $216 = 3 \cdot 55 + 51 \rightsquigarrow$ envia $c = 51$.
- Bob rep $c = 51$. Per desxifrar-ho, ha de fer l'arrel cúbica mod 55.
 - ▶ Resulta que en aritmètica modular, es pot calcular l'arrel cúbica elevant a un altre nombre. Pel cas de $N = 55$, cal elevar a $d = 27$.
 - ▶ Si fem 51^{27} i restem múltiples de 55 fins a caure entre 0 i 54 obtenim 6, que és el missatge original.
- Per què això és segur?
 - ▶ Per desxifrar el missatge, cal saber calcular arrels cúbiques mod N . Què evita que Eve pugui prendre una arrel cúbica mod N ?
 - ▶ Si N és molt gran, només es coneixen mètodes ràpids per a calcular arrels cúbiques si en coneixem els dos factors primers.

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - R  cord actual: factoritzar un producte de dos primers de 232 d  gits (equivalent a 2000 anys de c  lculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígit (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - Récord actual: factoritzar un producte de dos primers de 232 dígits (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - ▶ Récord actual: factoritzar un producte de dos primers de 232 dígit (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

RSA: exemple real

$p = 5311520355088381732434640236485900354436072788334240607719207689566489176525958810918512349859949112857361338219437970077582950526100742305335014064258231$

$q = 50096851814110051001251334144376270306245303522445016997030927250103665008535997628269932914411203856611856161140314779996692076749777532250263743482451$

$N = p \cdot q = 2660904481364918586560870876445438943393581321136249052667662004066060697383323989352781213580590828835783582555069362723931120892291823860125838775766191976115588331919553713790783987917465855715812885982682719755463990454715581532061176368517171986842788489126751367498522962441800564495982278934080804181$

- $N = p \cdot q$ té unes 300 xifres ($N \simeq 2.6 \times 10^{300}$)
- Com de gros és aquest nombre? Quant trigariem a factoritzar-lo?
- Hauríem provar unes 10^{150} operacions...
- Un ordinador avui en dia pot fer unes 10^{11} operacions per segon...
- Trigariem uns 10^{139} segons, que són $\sim 10^{131}$ anys...
- L'edat de l'univers és de 1.3×10^{10} anys!
- Això seria fent el mètode naïf, però hi ha mètodes més ràpids:
 - ▶ Récord actual: factoritzar un producte de dos primers de 232 dígit (equivalent a 2000 anys de càlculs en un processador a 2.2GHz)

L'amenaça quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic

L'amenaça quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic
- 1995: Peter Shor trobà un mètode ràpid amb un **ordinador quàntic**

L'amenaça quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic
 - 1995: Peter Shor trobà un mètode ràpid amb un **ordinador quàntic**
-
- ▶ Utilitza principis de la mecànica quàntica (superposició, entrellaçament) per a processar la informació
 - ▶ En comptes de bits (0's i 1's) utilitza qubits (superposicions de 0 i 1)
 - ▶ Funciona amb una lògica diferent, que permet resoldre certs problemes més ràpidament que amb ordinadors clàssics.



L'amenaça quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic
- 1995: Peter Shor trobà un mètode ràpid amb un **ordinador quàntic**
- ▶ Utilitza principis de la mecànica quàntica (superposició, entrellaçament) per a processar la informació
- ▶ En comptes de bits (0's i 1's) utilitza qubits (superposicions de 0 i 1)
- ▶ Funciona amb una lògica diferent, que permet resoldre certs problemes més ràpidament que amb ordinadors clàssics.
- El 1995 no hi havia ordinadors quàntics, avui ja n'hi ha alguns però no són prou potents encara per trencar RSA



L'amença quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic
- 1995: Peter Shor trobà un mètode ràpid amb un **ordinador quàntic**
- ▶ Utilitza principis de la mecànica quàntica (superposició, entrelaçament) per a processar la informació
- ▶ En comptes de bits (0's i 1's) utilitza qubits (superposicions de 0 i 1)
- ▶ Funciona amb una lògica diferent, que permet resoldre certs problemes més ràpidament que amb ordinadors clàssics.
- El 1995 no hi havia ordinadors quàntics, avui ja n'hi ha alguns però no són prou potents encara per trencar RSA
- Arribaran els ordinadors quàntics capaços de trencar RSA?



L'amenaça quàntica

- La seguretat a internet es basa en què no es coneix cap mètode ràpid per factoritzar enters grans...amb un ordinador clàssic
- 1995: Peter Shor trobà un mètode ràpid amb un **ordinador quàntic**
- ▶ Utilitza principis de la mecànica quàntica (superposició, entrelaçament) per a processar la informació
- ▶ En comptes de bits (0's i 1's) utilitza qubits (superposicions de 0 i 1)
- ▶ Funciona amb una lògica diferent, que permet resoldre certs problemes més ràpidament que amb ordinadors clàssics.
- El 1995 no hi havia ordinadors quàntics, avui ja n'hi ha alguns però no són prou potents encara per trencar RSA
- Arribaran els ordinadors quàntics capaços de trencar RSA?
- Els investigadors en criptografia busquen **xifrats postquàntics**



Per a saber-ne més

- Los códigos secretos, Simon Singh.
 - ▶ Llibre d'història de la criptografia. Cobreix tot el que hem vist i molt més de manera amena i entenedora.

Per a saber-ne més

- Los códigos secretos, Simon Singh.
 - ▶ Llibre d'història de la criptografia. Cobreix tot el que hem vist i molt més de manera amena i entenedora.
- https://www.simon Singh.net/The_Black_Chamber/
 - ▶ Pàgina web on podeu jugar a encriptar i desencriptar missatges. Té molts xifrats, els que hem vist i alguns que no...

Per a saber-ne més

- Los códigos secretos, Simon Singh.
 - ▶ Llibre d'història de la criptografia. Cobreix tot el que hem vist i molt més de manera amena i entenedora.
- https://www.simon Singh.net/The_Black_Chamber/
 - ▶ Pàgina web on podeu jugar a encriptar i desencriptar missatges. Té molts xifrats, els que hem vist i alguns que no...
- The imitation game (Descifrando Enigma)
 - ▶ pel·lícula del 2014 on s'explica la història d'Alan Turing i com va trencar el xifrat d'enigma.

Per a saber-ne més

- Los códigos secretos, Simon Singh.
 - ▶ Llibre d'història de la criptografia. Cobreix tot el que hem vist i molt més de manera amena i entenedora.
- https://www.simon Singh.net/The_Black_Chamber/
 - ▶ Pàgina web on podeu jugar a encriptar i desencriptar missatges. Té molts xifrats, els que hem vist i alguns que no...
- The imitation game (Descifrando Enigma)
 - ▶ pel·lícula del 2014 on s'explica la història d'Alan Turing i com va trencar el xifrat d'enigma.
- Videos sobre la màquina enigma de James Grime (googlejar: numberphile enigma)

Per a saber-ne més

- Los códigos secretos, Simon Singh.
 - ▶ Llibre d'història de la criptografia. Cobreix tot el que hem vist i molt més de manera amena i entenedora.
- https://www.simon Singh.net/The_Black_Chamber/
 - ▶ Pàgina web on podeu jugar a encriptar i desencriptar missatges. Té molts xifrats, els que hem vist i alguns que no...
- The imitation game (Descifrando Enigma)
 - ▶ pel·lícula del 2014 on s'explica la història d'Alan Turing i com va trencar el xifrat d'enigma.
- Videos sobre la màquina enigma de James Grime (googlejar: numberphile enigma)
- És un bon tema per a un treball de recerca!

Criptografia: les matemàtiques de la informació secreta

Xevi Guitart

Departament de Matemàtiques i Informàtica
Universitat de Barcelona