Introduction à la cryptographie

Elisa Gorla

Institut de mathématiques, Université de Neuchâtel

Colloque annuel de la Commission Romande de Mathématique
Leysin, 20 septembre 2017

Outline

❶ Brève histoire de la cryptographie

❷ La cryptographie moderne

❸ La cryptographie par courbes elliptiques

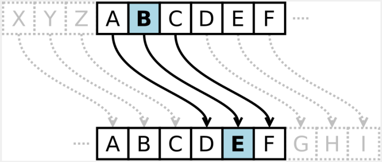
Brève histoire de la cryptographie

Chiffre de César

Le chiffrement par décalage a été utilisé par Jules César dans ses correspondances secrètes. Le texte chiffré s'obtient en remplaçant chaque lettre du texte original par une lettre située à k positions vers la droite dans l'ordre de l'alphabet.

Exemple

Avec un décalage de 3 vers la droite, on a



Donc le message "César" devient "Fhvdu".

Le destinataire peut déchiffrer le texte chiffré, s'il connait la clé secrète k.

Formulation mathématique

On a une correspondance entre les lettres de l'alphabet et les nombres $0, \ldots, 25$:

$$a \leftrightarrow 0, b \leftrightarrow 1, c \leftrightarrow 2, d \leftrightarrow 3, \ldots, y \leftrightarrow 24, z \leftrightarrow 25.$$

On ècrit $\mathbb{Z}_{26}$ pour les nombres $0, 1, \ldots, 25$ (où la somme est définie modulo 26) et $\mathbb{Z}_{26}^*$ pour les séquences d'elements de $\mathbb{Z}_{26}$ de longueur quelconque.

Formulation mathématique

On a une correspondance entre les lettres de l'alphabet et les nombres $0, \ldots, 25$:

$$a \leftrightarrow 0, b \leftrightarrow 1, c \leftrightarrow 2, d \leftrightarrow 3, \ldots, y \leftrightarrow 24, z \leftrightarrow 25.$$

On ècrit $\mathbb{Z}_{26}$ pour les nombres $0, 1, \ldots, 25$ (où la somme est définie modulo 26) et $\mathbb{Z}_{26}^*$ pour les séquences d'elements de $\mathbb{Z}_{26}$ de longueur quelconque.

La fonction de chiffrement du chiffre de César avec clé k est donc

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \ldots & \mapsto & x_1 + k, x_2 + k, x_3 + k, \ldots \end{array}$$

Cryptanalyse du chiffre de César

Même si on ne connait pas la clé secrète k, pour déchiffrer le message il suffit de tester tous les décalages possibles. C'est ce qu'on appelle une attaque par force brute, dont la complexité est le nombre des clés possibles.

Exemple

On a le message chiffré

"Qjx mtrrjx hwtnjsy atqtsynjwx hj vz'nqx ijxnwjsy".

Si on teste toutes les clés possibles, on obtient

k	message
1	Piw lsqqiw gvsmirx zspsrxmivw gi uy'mpw hiwmvirx

Cryptanalyse du chiffre de César

Même si on ne connait pas la clé secrète k, pour déchiffrer le message il suffit de tester tous les décalages possibles. C'est ce qu'on appelle une attaque par force brute, dont la complexité est le nombre des clés possibles.

Exemple

On a le message chiffré

"Qjx mtrrjx hwtnjsy atqtsynjwx hj vz'nqx ijxnwjsy".

Si on teste toutes les clés possibles, on obtient

k	message
1	Piw lsqqiw gvsmirx zspsrxmivw gi uy'mpw hiwmvirx
2	Ohv krpphv furlhqw yrorqwlhuv fh tx'lov ghvluhqw

Cryptanalyse du chiffre de César

Même si on ne connait pas la clé secrète k, pour déchiffrer le message il suffit de tester tous les décalages possibles. C'est ce qu'on appelle une attaque par force brute, dont la complexité est le nombre des clés possibles.

Exemple

On a le message chiffré

"Qjx mtrrjx hwtnjsy atqtsynjwx hj vz'nqx ijxnwjsy".

Si on teste toutes les clés possibles, on obtient

k	message
1	Piw lsqqiw gvsmirx zspsrxmivw gi uy'mpw hiwmvirx
2	Ohv krpphv furlhqw yrorqwlhuv fh tx'lov ghvluhqw
3	Ngu jqoogu etqkgpv xqnqpvkgtu eg sw'knu fguktgpv

Cryptanalyse du chiffre de César

Même si on ne connait pas la clé secrète k, pour déchiffrer le message il suffit de tester tous les décalages possibles. C'est ce qu'on appelle une attaque par force brute, dont la complexité est le nombre des clés possibles.

Exemple

On a le message chiffré

"Qjx mtrrjx hwtnjsy atqtsynjwx hj vz'nqx ijxnwjsy".

Si on teste toutes les clés possibles, on obtient

k	message
1	Piw lsqqiw gvsmirx zspsrxmivw gi uy'mpw hiwmvirx
2	Ohv krpphv furlhqw yrorqwlhuv fh tx'lov ghvluhqw
3	Ngu jqoogu etqkgpv xqnqpvkgtu eg sw'knu fguktgpv
4	Mft ipnnft dspjfou wpmpoujfst df rv'jmt eftjsfou

Cryptanalyse du chiffre de César

Même si on ne connait pas la clé secrète k, pour déchiffrer le message il suffit de tester tous les décalages possibles. C'est ce qu'on appelle une attaque par force brute, dont la complexité est le nombre des clés possibles.

Exemple

On a le message chiffré

"Qjx mtrrjx hwtnjsy atqtsynjwx hj vz'nqx ijxnwjsy".

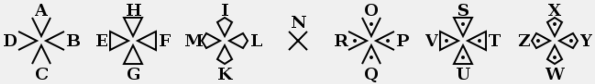
Si on teste toutes les clés possibles, on obtient

k	message
1	Piw lsqqiw gvsmirx zspsrxmivw gi uy'mpw hiwmvirx
2	Ohv krpphv furlhqw yrorqwlhuv fh tx'lov ghvluhqw
3	Ngu jqoogu etqkgpv xqnqpvkgtu eg sw'knu fguktgpv
4	Mft ipnnft dspjfou wpmpoujfst df rv'jmt eftjsfou
5	Les hommes croient volontiers ce qu'ils désirent

Chiffrement par substitution

Le chiffrement par substitution consiste à substituer dans un message chacune des lettres de l'alphabet par une autre lettre ou symbole fixé (substitution monoalphabétique) ou par une autre lettre choisie en fonction d'un état du cryptosystème (substitution polyalphabétique).

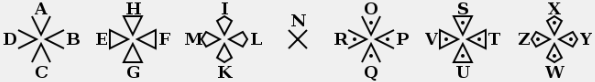
Exemple (Chiffre des Templiers (XIII-ème siècle))



Chiffrement par substitution

Le chiffrement par substitution consiste à substituer dans un message chacune des lettres de l'alphabet par une autre lettre ou symbole fixé (substitution monoalphabétique) ou par une autre lettre choisie en fonction d'un état du cryptosystème (substitution polyalphabétique).

Exemple (Chiffre des Templiers (XIII-ème siècle))

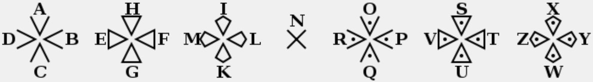


La complexité d'une attaque par force brute à une chiffrement par substitution monoalphabétique est le nombre des permutations des 26 lettres, donc $26 \cdot 25 \cdots 2 \cdot 1 = 26! \sim 4,03 \cdot 10^{26} \sim 1,30 \cdot 2^{88}$.

Chiffrement par substitution

Le chiffrement par substitution consiste à substituer dans un message chacune des lettres de l'alphabet par une autre lettre ou symbole fixé (substitution monoalphabétique) ou par une autre lettre choisie en fonction d'un état du cryptosystème (substitution polyalphabétique).

Exemple (Chiffre des Templiers (XIII-ème siècle))



La complexité d'une attaque par force brute à une chiffrement par substitution monoalphabétique est le nombre des permutations des 26 lettres, donc $26 \cdot 25 \cdots 2 \cdot 1 = 26! \sim 4,03 \cdot 10^{26} \sim 1,30 \cdot 2^{88}$.
Les chiffrements utilisant la substitution monoalphabétique sont faciles à casser par analyse fréquentielle.

Analyse fréquentielle

lettre	fréquence	lettre	fréquence
a	8,25	n	7,25
b	1,25	o	5,75
c	3,25	p	3,75
d	3,75	q	1,25
e	17,75	r	7,25
f	1,25	s	8,25
g	1,25	t	7,25
h	1,25	u	6,25
i	7,25	v	1,75
j	0,75	w	0,00
k	0,00	x	0,00
l	5,75	y	0,75
m	3,25	z	0,00

1. L'analyse
des fréquences dans le texte
chiffré nous permet d'établir
une correspondance entre les
lettres les plus fréquentes.
2. On remplace
les lettres dans le texte
suivant cette correspondance
et on voi si ça marche.
3. On peut aussi utilizer
la fréquence d'apparition
des bigrammes (couple
de lettres) pour deviner
des autres correspondances.
4. On répéte si necessaire.

Le chiffre de Vigenère (XVI-ème siècle)

Le chiffrement de Vigenère ressemble beaucoup au chiffrement de César, la difference étant que on utilise un mot clé au lieu d'un seul caractère (la clé étant répétée autant de fois que nécessaire).

Exemple

Chiffrement du message "Attaquer à l'aube" avec clé "axfre" :

A	T	T	A	Q	U	E	R	A	L	A	U	B	E
A 0	X 23	F 5	R 17	E 4	A 0	X 23	F 5	R 17	E 4	A 0	X 23	F 5	R 17
A	Q	Y	R	U	U	B	W	R	P	A	R	G	V

Le chiffre de Vigenère (XVI-ème siècle)

Le chiffrement de Vigenère ressemble beaucoup au chiffrement de César, la difference étant que on utilise un mot clé au lieu d'un seul caractère (la clé étant répétée autant de fois que nécessaire).

Exemple

Chiffrement du message "Attaquer à l'aube" avec clé "axfre" :

A	T	T	A	Q	U	E	R	A	L	A	U	B	E
A 0	X 23	F 5	R 17	E 4	A 0	X 23	F 5	R 17	E 4	A 0	X 23	F 5	R 17
A	Q	Y	R	U	U	B	W	R	P	A	R	G	V

La fonction de chiffrement du chiffre de Vigenère est donc

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^n & \longrightarrow & \mathbb{Z}_{26}^n \\ (x_1, x_2 \ldots, x_n) & \mapsto & (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n) \end{array}$$

où la clé est $(k_1, k_2, \ldots, k_n)$ de longueur n.

Cryptanalyse du chiffre de Vigenère

En supposant la longueur n de la clé connue, un message peut être décrypté facilement de la façon suivante :

1. Décomposer le texte chiffré en n textes : le premier texte est la suite des lettres en positions $1, n+1, 2n+1, 3n+1, \ldots$, le deuxième est la suite des lettres en positions $2, n+2, 2n+2, 3n+2, \ldots$ et ainsi de suite.

Cryptanalyse du chiffre de Vigenère

En supposant la longueur n de la clé connue, un message peut être décrypté facilement de la façon suivante :

1. Décomposer le texte chiffré en n textes : le premier texte est la suite des lettres en positions $1, n+1, 2n+1, 3n+1, \ldots$, le deuxième est la suite des lettres en positions $2, n+2, 2n+2, 3n+2, \ldots$ et ainsi de suite.

2. Chaque texte est chiffré comme dans le chiffre de César (avec des clés differents)

Cryptanalyse du chiffre de Vigenère

En supposant la longueur n de la clé connue, un message peut être décrypté facilement de la façon suivante :

1. Décomposer le texte chiffré en n textes : le premier texte est la suite des lettres en positions $1, n+1, 2n+1, 3n+1, \ldots$, le deuxième est la suite des lettres en positions $2, n+2, 2n+2, 3n+2, \ldots$ et ainsi de suite.

2. Chaque texte est chiffré comme dans le chiffre de César (avec des clés differents) $\rightsquigarrow$ l'analyse fréquentielle nous permet de décrypter chacun des n textes.

Cryptanalyse du chiffre de Vigenère

En supposant la longueur n de la clé connue, un message peut être décrypté facilement de la façon suivante :

1. Décomposer le texte chiffré en n textes : le premier texte est la suite des lettres en positions $1, n+1, 2n+1, 3n+1, \ldots$, le deuxième est la suite des lettres en positions $2, n+2, 2n+2, 3n+2, \ldots$ et ainsi de suite.

2. Chaque texte est chiffré comme dans le chiffre de César (avec des clés differents) $\rightsquigarrow$ l'analyse fréquentielle nous permet de décrypter chacun des n textes.

3. Recomposer les n textes ainsi décryptés pour composer le message d'origine.

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA
- QBR

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA
- QBR
- YWG

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA
- QBR
- YWG
- RRV

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA
- QBR
- YWG
- RRV
- UP

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA $\rightsquigarrow$ AUA avec clé A
- QBR $\rightsquigarrow$ TEU avec clé X
- YWG $\rightsquigarrow$ TRB avec clé F
- RRV $\rightsquigarrow$ AAE avec clé R
- UP $\rightsquigarrow$ QL avec clé E

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA $\rightsquigarrow$ AUA avec clé A
- QBR $\rightsquigarrow$ TEU avec clé X
- YWG $\rightsquigarrow$ TRB avec clé F
- RRV $\rightsquigarrow$ AAE avec clé R
- UP $\rightsquigarrow$ QL avec clé E

donc ATTAQ

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA $\rightsquigarrow$ AUA avec clé A
- QBR $\rightsquigarrow$ TEU avec clé X
- YWG $\rightsquigarrow$ TRB avec clé F
- RRV $\rightsquigarrow$ AAE avec clé R
- UP $\rightsquigarrow$ QL avec clé E

donc ATTAQUERAL

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA $\rightsquigarrow$ AUA avec clé A
- QBR $\rightsquigarrow$ TEU avec clé X
- YWG $\rightsquigarrow$ TRB avec clé F
- RRV $\rightsquigarrow$ AAE avec clé R
- UP $\rightsquigarrow$ QL avec clé E

donc ATTAQUERALAUBE.

Cryptanalyse du chiffre de Vigenère – exemple

Le texte chiffré A Q Y R U U B W R P A R G V avec clé de longueur 5 donne les 5 textes chiffrés :

- AUA $\rightsquigarrow$ AUA avec clé A
- QBR $\rightsquigarrow$ TEU avec clé X
- YWG $\rightsquigarrow$ TRB avec clé F
- RRV $\rightsquigarrow$ AAE avec clé R
- UP $\rightsquigarrow$ QL avec clé E

donc ATTAQUERALAUBE.

Question

Comment calculer la longueur de la clé ?

Cryptanalyse du chiffre de Vigenère – le test de Kasiski (1863)

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

Cryptanalyse du chiffre de Vigenère – le test de Kasiski (1863)

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

Cryptanalyse du chiffre de Vigenère – le test de Kasiski (1863)

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

séquence répétée	distance entre les répetitions
WUU	95
EEK	200
WXIZAYG	190
NUOCZGM	80
DOEOY	45
GMU	90

Cryptanalyse du chiffre de Vigenère – le test de Kasiski (1863)

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

séquence répétée	distance entre les répetitions
WUU	95
EEK	200
WXIZAYG	190
NUOCZGM	80
DOEOY	45
GMU	90

$\text{PGDC}(95, 200, 190, 80, 45, 90) = 5$, donc la clé a longueur 5.

Récapitulation: test de Kasiski et cryptanalyse du chiffre de Vigenère

Pour calculer la longueur de la clé à partir du texte chiffré :

- On cherche les répétitions dans le texte chiffré et on calcule la distance entre chaque paire de séquences identiques consécutives.
- Le plus grand denominateur commun entre les distances est (un multiple de) la longueur de la clé.

Récapitulation: test de Kasiski et cryptanalyse du chiffre de Vigenère

Pour calculer la longueur de la clé à partir du texte chiffré :

- On cherche les répétitions dans le texte chiffré et on calcule la distance entre chaque paire de séquences identiques consécutives.
- Le plus grand denominateur commun entre les distances est (un multiple de) la longueur de la clé.

Pour déchiffrer un texte chiffré avec le cryptosystème de Vigenère :

- On calcule la longueur n de la clé.
- On décompose le texte chiffré en n textes.
- On déchiffre chaque texte chiffré en utilisant l'analyse fréquentielle.
- On recompose le message d'origine à partir des n textes dechiffrés.

Récapitulation: test de Kasiski et cryptanalyse du chiffre de Vigenère

Pour calculer la longueur de la clé à partir du texte chiffré :

- On cherche les répétitions dans le texte chiffré et on calcule la distance entre chaque paire de séquences identiques consécutives.
- Le plus grand denominateur commun entre les distances est (un multiple de) la longueur de la clé.

Pour déchiffrer un texte chiffré avec le cryptosystème de Vigenère :

- On calcule la longueur n de la clé.
- On décompose le texte chiffré en n textes.
- On déchiffre chaque texte chiffré en utilisant l'analyse fréquentielle.
- On recompose le message d'origine à partir des n textes dechiffrés.

Remarque

L'analyse fréquentielle fonctionne, même si le texte original n'a pas de sens.
À comparer avec une attaque par force brute, qui exige 26^n tentatives.

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \dots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \dots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \dots \end{array}$$

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \dots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \dots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \dots \end{array}$$

Exemple

m	e	s	s	a	g	e	c	l	a	i	r
a 0	s 18	e 4	t 19	x 23	c 2	w 22	l 11	m 12	o 14	z 25	a 0
m	w	w	k	x	i	a	n	x	p	h	r

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \ldots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \ldots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots \end{array}$$

Le chiffre de Vernam est théoriquement impossible à casser, c.-à-d.

$$p(x|y) = p(x) \quad \forall x, y$$

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \ldots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \ldots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots \end{array}$$

Le chiffre de Vernam est théoriquement impossible à casser, c.-à-d.

$$p(x|y) = p(x) \quad \forall x, y$$

mais il présente d'importantes difficultés de mise en œuvre :

- la clé doit être aussi longue que le message à chiffrer,

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \ldots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \ldots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots \end{array}$$

Le chiffre de Vernam est théoriquement impossible à casser, c.-à-d.

$$p(x|y) = p(x) \quad \forall x, y$$

mais il présente d'importantes difficultés de mise en œuvre :

- la clé doit être aussi longue que le message à chiffrer,
- les caractères composant la clé doivent être choisis de façon aléatoire,

Le chiffre de Vernam (1917)

On déplace la premiere lettre du text original de k_1 positions vers la droite, la deuxième de k_2 positions, la troisième de k_3 positions, etc. où $k_1, k_2, k_3, \ldots$ sont nombres aléatoires choisis à nouveau pour chaque transmission.
Pour chaque clé $k \in \mathbb{Z}_{26}^*$ on a donc la fonction de chiffrement

$$\begin{array}{rcl} f : \mathbb{Z}_{26}^* & \longrightarrow & \mathbb{Z}_{26}^* \\ x_1, x_2, x_3, \ldots & \mapsto & x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots \end{array}$$

Le chiffre de Vernam est théoriquement impossible à casser, c.-à-d.

$$p(x|y) = p(x) \quad \forall x, y$$

mais il présente d'importantes difficultés de mise en œuvre :

- la clé doit être aussi longue que le message à chiffrer,
- les caractères composant la clé doivent être choisis de façon aléatoire,
- chaque clé ne doit être utilisée qu'une seule fois.

La cryptographie moderne

La cryptographie aujourd'hui

La cryptographie est la pratique et l'étude de méthodes pour assurer la confidentialité des messages. Elle nous permet de stocker des informations sensibles ou de les transmettre dans des réseaux non sécurisés (par exemple l'Internet) de sorte qu'elles ne peuvent être lues par quiconque, sauf le destinataire.

La cryptographie aujourd'hui

La cryptographie est la pratique et l'étude de méthodes pour assurer la confidentialité des messages. Elle nous permet de stocker des informations sensibles ou de les transmettre dans des réseaux non sécurisés (par exemple l'Internet) de sorte qu'elles ne peuvent être lues par quiconque, sauf le destinataire.

La cryptographie s'occupe de :

- authentification : prouver son identité,
- confidentialité : personne ne peut lire le message, à l'exception du destinataire,
- intégrité des données : le destinataire peut verifier que le message n'a pas été modifié,
- non-répudiation : prouver que l'expéditeur a vraiment envoyé un message donné.

Le principe de Kerckhoffs (1883)

JOURNAL DES SCIENCES MILITAIRES.

II.

DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Tout le monde est d'accord pour admettre la raison d'être des

La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé. Tous les autres paramètres doivent être supposés publiquement connus.

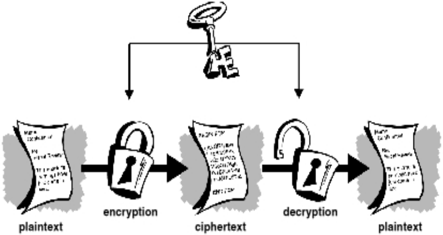
Pas de sécurité par l'obscurité

ou

L'adversaire connaît le système (Claude Shannon)

Deux types d'algorithmes cryptographiques

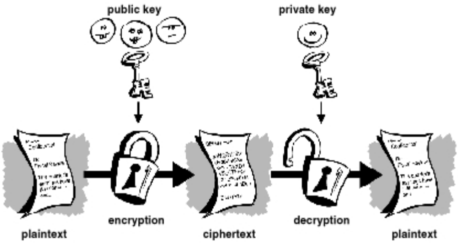
Dans la cryptographie à clé secrète on utilise la même clé pour chiffrer et déchiffrer un message. La difficulté principale est que les parties qui communiquent doivent s'accorder sur une clé secrète commune, en communiquant sur un réseau public.



Deux types d'algorithmes cryptographiques

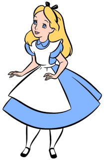
Dans la cryptographie à clé secrète on utilise la même clé pour chiffrer et déchiffrer un message. La difficulté principale est que les parties qui communiquent doivent s'accorder sur une clé secrète commune, en communiquant sur un réseau public.

Dans la cryptographie à clé publique on utilise deux clés, une clé publique, permettant le chiffrement, et une clé privée, permettant le déchiffrement.



L'idée de la cryptographie à clé publique

Bob

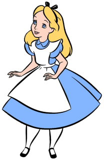


Alice

L'idée de la cryptographie à clé publique

Bob

Eve

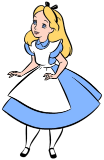


Alice

L'idée de la cryptographie à clé publique

Bob

Eve

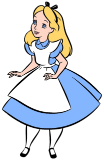


Alice

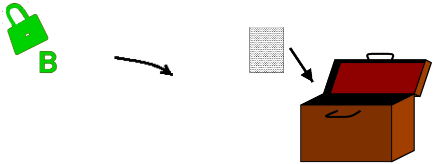
L'idée de la cryptographie à clé publique

Bob

Eve



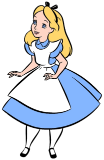
Alice



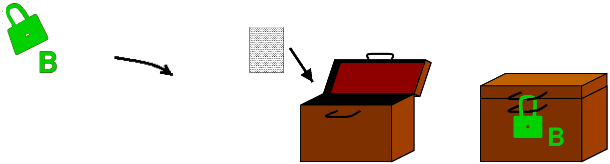
L'idée de la cryptographie à clé publique

Bob

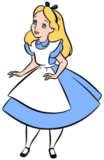
Eve



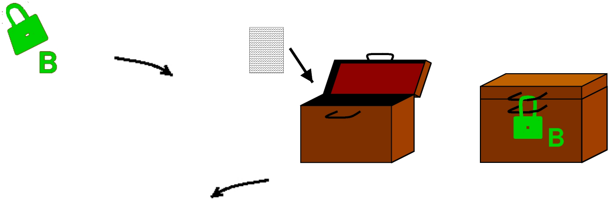
Alice



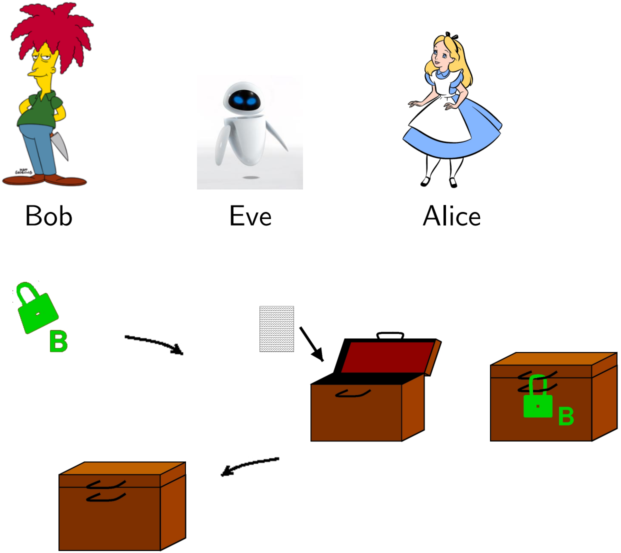
L'idée de la cryptographie à clé publique



Bob Eve Alice



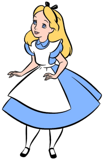
L'idée de la cryptographie à clé publique



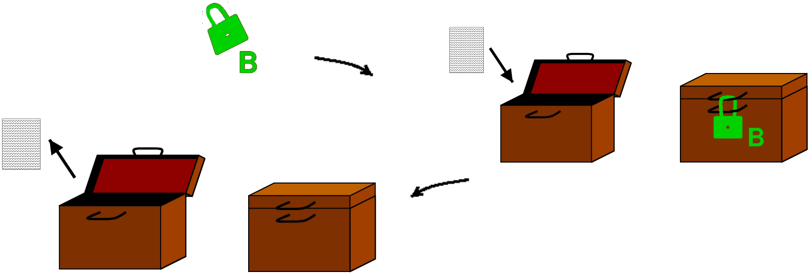
L'idée de la cryptographie à clé publique

Bob

Eve



Alice



Exemple – le chiffrement RSA (1977)

Bob choisit deux nombres premiers $p, q \sim 10^{150}$ et il calcule $n = pq$. Il choisit un nombre $e < n$ aléatoire t.q. e et $\phi = (p-1)(q-1)$ sont premier entre eux. Sa fonction de cryptage est

$$\begin{aligned} f : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ m &\longmapsto m^e = c \end{aligned}$$

Bob utilize l'algorithme de Euclide pour calculer $d, b \in \mathbb{Z}$ t.q. $de + b\phi = 1$.

Exemple – le chiffrement RSA (1977)

Bob choisit deux nombres premiers $p, q \sim 10^{150}$ et il calcule $n = pq$. Il choisit un nombre $e < n$ aléatoire t.q. e et $\phi = (p-1)(q-1)$ sont premier entre eux. Sa fonction de cryptage est

$$\begin{aligned} f : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ m &\longmapsto m^e = c \end{aligned}$$

Bob utilize l'algorithme de Euclide pour calculer $d, b \in \mathbb{Z}$ t.q. $de + b\phi = 1$. Sa clé publique est (e, n) et sa clé privée est (d, ϕ) et

$$\begin{aligned} f^{-1} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ c &\longmapsto c^d = m^{ed} = m^{1-b\phi} = m. \end{aligned}$$

Exemple – le chiffrement RSA (1977)

Bob choisit deux nombres premiers $p, q \sim 10^{150}$ et il calcule $n = pq$. Il choisit un nombre $e < n$ aléatoire t.q. e et $\phi = (p-1)(q-1)$ sont premier entre eux. Sa fonction de cryptage est

$$\begin{aligned} f : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ m &\longmapsto m^e = c \end{aligned}$$

Bob utilize l'algorithme de Euclide pour calculer $d, b \in \mathbb{Z}$ t.q. $de + b\phi = 1$. Sa clé publique est (e, n) et sa clé privée est (d, ϕ) et

$$\begin{aligned} f^{-1} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ c &\longmapsto c^d = m^{ed} = m^{1-b\phi} = m. \end{aligned}$$

Remarques

Factorizer n est computationnellement équivalent à calculer d.

La méthode connue la plus rapide pour calculer m à partir de c est factorizer n.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.
La fonction s'appelle à brèche secrète si il est possible trouver m de c en ayant la clé privée.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.
La fonction s'appelle à brèche secrète si il est possible trouver m de c en ayant la clé privée.

Comment ça marche :

1. Bob construit une fonction à brèche secrète $f : M \longrightarrow C$ et la publie.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.
La fonction s'appelle à brèche secrète si il est possible trouver m de c en ayant la clé privée.

Comment ça marche :

1. Bob construit une fonction à brèche secrète $f : M \longrightarrow C$ et la publie.
2. Alice veut envoyer le message $m \in M$ à Bob. Elle calcule et envoie $f(m) = c$ à Bob.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.
La fonction s'appelle à brèche secrète si il est possible trouver m de c en ayant la clé privée.

Comment ça marche :

1. Bob construit une fonction à brèche secrète $f : M \longrightarrow C$ et la publie.
2. Alice veut envoyer le message $m \in M$ à Bob. Elle calcule et envoie $f(m) = c$ à Bob.
3. Seulement Bob peut calculer $m = f^{-1}(c)$.

Fonctions à sens unique

Définition

Une fonction à sens unique est une fonction $f : M \longrightarrow C$ qui peut être aisément calculée, mais qui est très difficile à inverser.
C'est-à-dire que, étant donné un texte chiffré $c \in C$, il est pratiquement impossible de trouver le message $m \in M$ t.q. $f(m) = c$.
La fonction s'appelle à brèche secrète si il est possible trouver m de c en ayant la clé privée.

Comment ça marche :

1. Bob construit une fonction à brèche secrète $f : M \longrightarrow C$ et la publie.
2. Alice veut envoyer le message $m \in M$ à Bob. Elle calcule et envoie $f(m) = c$ à Bob.
3. Seulement Bob peut calculer $m = f^{-1}(c)$.

Les fonctions à brèche secrète utilisent des problèmes mathématiques qui ne peuvent pas être résolus pratiquement. Notre système cryptographique est donc sûr, si le problème mathématique correspondant est difficile.

Exemples de problèmes difficiles

1. factorisation : Calculer le produit $n = p * q$ de deux nombres premiers p et q est facile, même s'ils sont très grands. Par contre, calculer p et q à partir de n est difficile.

Exemples de problèmes difficiles

1. factorisation : Calculer le produit $n = p * q$ de deux nombres premiers p et q est facile, même s'ils sont très grands. Par contre, calculer p et q à partir de n est difficile.
2. logarithme discret : On appelle groupe un ensemble muni d'une opération $*$. Le logarithme discret de Q dans la base P est un nombre ℓ t.q.

$$\underbrace{P * P * \cdots * P}_{\ell \text{ fois}} = P^\ell = Q.$$

   Calculer le produit P^ℓ est facile, mais calculer $\ell = \log_P(Q)$ à partir de P et Q est difficile en général.

Exemple (le logarithme usuel)

Si P et Q sont des nombres entiers, on a le logarithme usuel. Par exemple $\log_3 81 = 4$ car $3^4 = 81$. Le logarithme usuel est facile à calculer.

Exemples de problèmes difficiles

1. factorisation : Calculer le produit $n = p * q$ de deux nombres premiers p et q est facile, même s'ils sont très grands. Par contre, calculer p et q à partir de n est difficile.
2. logarithme discret : On appelle groupe un ensemble muni d'une opération $*$. Le logarithme discret de Q dans la base P est un nombre ℓ t.q.

$$\underbrace{P * P * \cdots * P}_{\ell \text{ fois}} = P^\ell = Q.$$

   Calculer le produit P^ℓ est facile, mais calculer $\ell = \log_P(Q)$ à partir de P et Q est difficile en général.

Problème du logarithme discret (PLD)

Soit G un groupe fini, $P, Q \in G$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

Le chiffrement ElGamal (1984)

Soit $(G = \langle P \rangle, *)$ un groupe cyclique fini engendré par P, c.-à-d., tous les éléments de G sont de la forme P^m.
Bob choisit un nombre aléatoire ℓ et il calcule $Q = P^\ell$.
La fonction à brèche secrète de Bob est

$$\begin{array}{rcl} f_k : G & \longrightarrow & G \times G \\ M & \longmapsto & (P^k, M * Q^k) = (C_1, C_2) \end{array}$$

où k est un entier aléatoire choisi par Alice.

Le chiffrement ElGamal (1984)

Soit $(G = \langle P \rangle, *)$ un groupe cyclique fini engendré par P, c.-à-d., tous les éléments de G sont de la forme P^m.
Bob choisit un nombre aléatoire ℓ et il calcule $Q = P^\ell$.
La fonction à brèche secrète de Bob est

$$\begin{array}{rcl} f_k : G & \longrightarrow & G \times G \\ M & \longmapsto & (P^k, M * Q^k) = (C_1, C_2) \end{array}$$

où k est un entier aléatoire choisi par Alice.

Clé publique : $P, Q \in G$.

Le chiffrement ElGamal (1984)

Soit $(G = \langle P \rangle, *)$ un groupe cyclique fini engendré par P, c.-à-d., tous les éléments de G sont de la forme P^m.
Bob choisit un nombre aléatoire ℓ et il calcule $Q = P^\ell$.
La fonction à brèche secrète de Bob est

$$\begin{aligned} f_k : G &\longrightarrow G \times G \\ M &\longmapsto (P^k, M * Q^k) = (C_1, C_2) \end{aligned}$$

où k est un entier aléatoire choisi par Alice.

Clé publique : $P, Q \in G$. Clé privée : ℓ.

Bob connait ℓ, donc il peut calculer

$$M = f_k^{-1}(C_1, C_2) = C_2 * C_1^{-\ell}.$$

Le chiffrement ElGamal (1984)

Soit $(G = \langle P \rangle, *)$ un groupe cyclique fini engendré par P, c.-à-d., tous les éléments de G sont de la forme P^m.
Bob choisit un nombre aléatoire ℓ et il calcule $Q = P^{\ell}$.
La fonction à brèche secrète de Bob est

$$\begin{array}{rcl} f_k : G & \longrightarrow & G \times G \\ M & \longmapsto & (P^k, M * Q^k) = (C_1, C_2) \end{array}$$

où k est un entier aléatoire choisi par Alice.

Clé publique : $P, Q \in G$. Clé privée : ℓ.

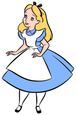
Bob connait ℓ, donc il peut calculer

$$M = f_k^{-1}(C_1, C_2) = C_2 * C_1^{-\ell}.$$

Si Eve peut résoudre le PLD, alors elle peut calculer ℓ.

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.



Alice

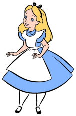
Eve

Bob

P

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.



Alice

Eve

Bob

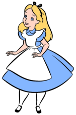
P

clé privée $a \in \mathbb{Z}$

clé privée $b \in \mathbb{Z}$

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.



Alice

Eve

Bob

P

clé privée $a \in \mathbb{Z}$

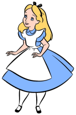
clé privée $b \in \mathbb{Z}$

clé publique P^a

clé publique P^b

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.



Alice

Eve

Bob

P

clé privée $a \in \mathbb{Z}$

clé privée $b \in \mathbb{Z}$

clé publique P^a

clé publique P^b

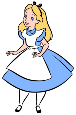
$(P^b)^a$

$(P^a)^b$

Clé secrète commune : $K = P^{ab}$.

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.



Alice

Eve

Bob

P

clé privée $a \in \mathbb{Z}$

clé privée $b \in \mathbb{Z}$

clé publique P^a

clé publique P^b

$(P^b)^a$

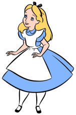
$(P^a)^b$

Clé secrète commune : $K = P^{ab}$.

Probleme de Diffie-Hellman : Eve connait P, P^a et P^b. Elle veut calculer P^{ab}.

Echange de clé de Diffie-Hellman (1976)

Situation : Alice et Bob veulent se mettre d'accord sur une clé secrète commune. La communication se fait entièrement en public.

Alice	Eve	Bob
		
Alice	Eve	Bob
	$P = 3$	
clé privée $a \in \mathbb{Z}$		clé privée $b \in \mathbb{Z}$
	clé publique $P^a = 81$ clé publique $P^b = 27$	
$(P^b)^a$		$(P^a)^b$

Clé secrète commune : $K = P^{ab}$.

Probleme de Diffie-Hellman : Eve connait P, P^a et P^b. Elle veut calculer P^{ab}.

La securité de l'echange de clé de DH

Problème de Diffie-Hellman (PDH)

Soit G un groupe fini, $a, b \in \mathbb{Z}$. Calculer P^{ab} à partir de P, P^a et P^b.

La securité de l'echange de clé de DH

Problème de Diffie-Hellman (PDH)

Soit G un groupe fini, $a, b \in \mathbb{Z}$. Calculer P^{ab} à partir de P, P^a et P^b.

Problème du logarithme discret (PLD)

Soit G un groupe fini, $P, Q \in G$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

La securité de l'echange de clé de DH

Problème de Diffie-Hellman (PDH)

Soit G un groupe fini, $a, b \in \mathbb{Z}$. Calculer P^{ab} à partir de P, P^a et P^b.

Problème du logarithme discret (PLD)

Soit G un groupe fini, $P, Q \in G$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

Le PDH peut être réduit au PLD, c.-à.-d.

$$\text{PDH} \leq \text{PLD}.$$

En fait, si Eve peut calculer b à partir de P et P^b, alors elle peut calculer $P^{ab} = (P^a)^b$. Alors le PLD est au moins aussi difficile que le PDH.

La securité de l'echange de clé de DH

Problème de Diffie-Hellman (PDH)

Soit G un groupe fini, $a, b \in \mathbb{Z}$. Calculer P^{ab} à partir de P, P^a et P^b.

Problème du logarithme discret (PLD)

Soit G un groupe fini, $P, Q \in G$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

Le PDH peut être réduit au PLD, c.-à.-d.

$$\text{PDH} \leq \text{PLD}.$$

En fait, si Eve peut calculer b à partir de P et P^b, alors elle peut calculer $P^{ab} = (P^a)^b$. Alors le PLD est au moins aussi difficile que le PDH.

Question ouverte

Est-ce que PDH $\geq$ PLD ?

La théorie de la complexité ou comment mesurons-nous la difficulté d'un problème ?

• Pour mesurer la complexité d'un algorithme dans un groupe G, on compte le nombre d'opérations effectuées par l'algorithme en fonction de $\log n$, où $n = |G|$.

Remarque

$\log_2 n$ est le nombre de bits nécessaires pour représenter n objets.

La théorie de la complexité ou comment mesurons-nous la difficulté d'un problème ?

• Pour mesurer la complexité d'un algorithme dans un groupe G, on compte le nombre d'opérations effectuées par l'algorithme en fonction de $\log n$, où $n = |G|$.

Remarque

$\log_2 n$ est le nombre de bits nécessaires pour représenter n objets.

• La complexité d'un problème est (au plus) la complexité de l'algorithme le plus efficace que nous connaissons pour le résoudre.

La théorie de la complexité ou comment mesurons-nous la difficulté d'un problème ?

• Pour mesurer la complexité d'un algorithme dans un groupe G, on compte le nombre d'opérations effectuées par l'algorithme en fonction de $\log n$, où $n = |G|$.

Remarque

$\log_2 n$ est le nombre de bits nécessaires pour représenter n objets.

• La complexité d'un problème est (au plus) la complexité de l'algorithme le plus efficace que nous connaissons pour le résoudre.
• Le crible général de corps de nombres est l'algorithm le plus efficace pour factorizer un nombre n et a complexité $\mathcal{O}\left(e^{\left(\frac{64}{9}\log n\right)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$.

La théorie de la complexité ou comment mesurons-nous la difficulté d'un problème ?

• Pour mesurer la complexité d'un algorithme dans un groupe G, on compte le nombre d'opérations effectuées par l'algorithme en fonction de $\log n$, où $n = |G|$.

Remarque

$\log_2 n$ est le nombre de bits nécessaires pour représenter n objets.

• La complexité d'un problème est (au plus) la complexité de l'algorithme le plus efficace que nous connaissons pour le résoudre.
• Le crible général de corps de nombres est l'algorithm le plus efficace pour factorizer un nombre n et a complexité $\mathcal{O}\left(e^{\left(\frac{64}{9}\log n\right)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$.
• L'algorithme rho de Pollard est le plus efficace pour calculer un logarithme discret et a complexité $\mathcal{O}(\sqrt{n}) = \mathcal{O}(e^{\frac{1}{2}\log n})$.

La cryptographie par courbes elliptiques

Courbes elliptiques

Soit p un nombre premier, $p > 3$. $\mathbb{Z}_p$ est un corps avec p éléments, c.-à.-d., chaque element a un invers multiplicatif.

Exemple (p=7)

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ et $2^{-1} = 4$ (car $2 * 4 = 1$), $3^{-1} = 5$.

Courbes elliptiques

Soit p un nombre premier, $p > 3$. $\mathbb{Z}_p$ est un corps avec p éléments, c.-à.-d., chaque element a un invers multiplicatif.

Exemple (p=7)

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ et $2^{-1} = 4$ (car $2 * 4 = 1$), $3^{-1} = 5$.

Définition

Une courbe elliptique E est définie par une équation de la forme $y^2 = f(x)$ où $f(x) \in \mathbb{Z}_p$ a degré 3 et racines simples.

Courbes elliptiques

Soit p un nombre premier, $p > 3$. $\mathbb{Z}_p$ est un corps avec p éléments, c.-à.-d., chaque element a un invers multiplicatif.

Exemple (p=7)

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ et $2^{-1} = 4$ (car $2 * 4 = 1$), $3^{-1} = 5$.

Définition

Une courbe elliptique E est définie par une équation de la forme $y^2 = f(x)$ où $f(x) \in \mathbb{Z}_p$ a degré 3 et racines simples.

Exemple

L'équation $y^2 = x^3 + x + 1$ définit une courbe elliptique sur $\mathbb{Z}_7$.

Le groupe des points d'une courbe elliptique

Définition

Le groupe des points de la courbe elliptique E sur $\mathbb{Z}_p$ est

$$E(\mathbb{Z}_p) = \{(a, b) \in \mathbb{Z}_p^2 \mid b^2 = f(a)\} \cup \{\mathcal{O}\}.$$

$\mathcal{O}$ est le point à l'infini de E, t.q. $P * \mathcal{O} = P$ pour chaque $P \in E(\mathbb{Z}_p)$.

Le groupe des points d'une courbe elliptique

Définition

Le groupe des points de la courbe elliptique E sur $\mathbb{Z}_p$ est

$$E(\mathbb{Z}_p) = \{(a, b) \in \mathbb{Z}_p^2 \mid b^2 = f(a)\} \cup \{\mathcal{O}\}.$$

$\mathcal{O}$ est le point à l'infini de E, t.q. $P * \mathcal{O} = P$ pour chaque $P \in E(\mathbb{Z}_p)$.

Exemple

Soit E la courbe d'équation $y^2 = x^3 + x + 1$ sur $\mathbb{Z}_7$.
Alors $E(\mathbb{Z}_7) = \{(0, 1), (0, 6), (2, 2), (2, 5), \mathcal{O}\}$.

Le groupe des points d'une courbe elliptique

Définition

Le groupe des points de la courbe elliptique E sur $\mathbb{Z}_p$ est

$$E(\mathbb{Z}_p) = \{(a, b) \in \mathbb{Z}_p^2 \mid b^2 = f(a)\} \cup \{\mathcal{O}\}.$$

$\mathcal{O}$ est le point à l'infini de E, t.q. $P * \mathcal{O} = P$ pour chaque $P \in E(\mathbb{Z}_p)$.

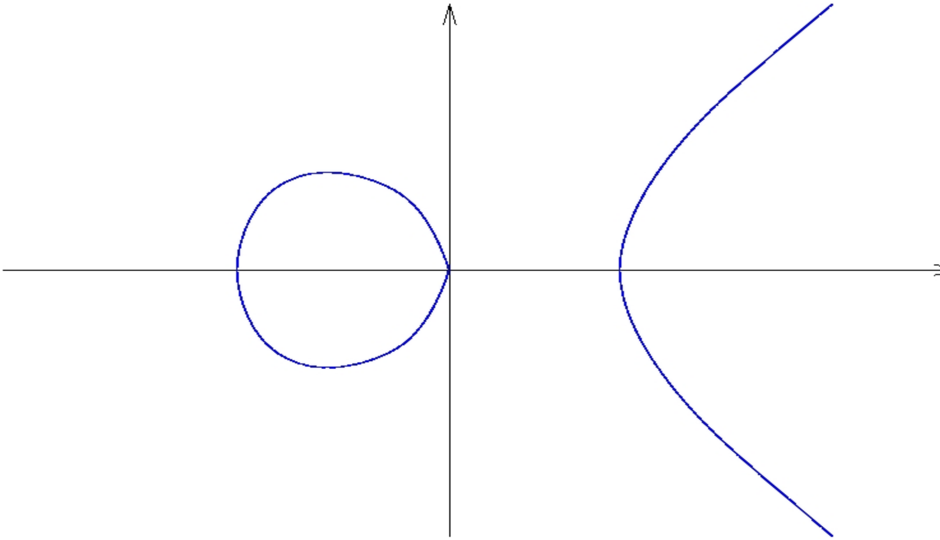
Exemple

Soit E la courbe d'équation $y^2 = x^3 + x + 1$ sur $\mathbb{Z}_7$.
Alors $E(\mathbb{Z}_7) = \{(0, 1), (0, 6), (2, 2), (2, 5), \mathcal{O}\}$.

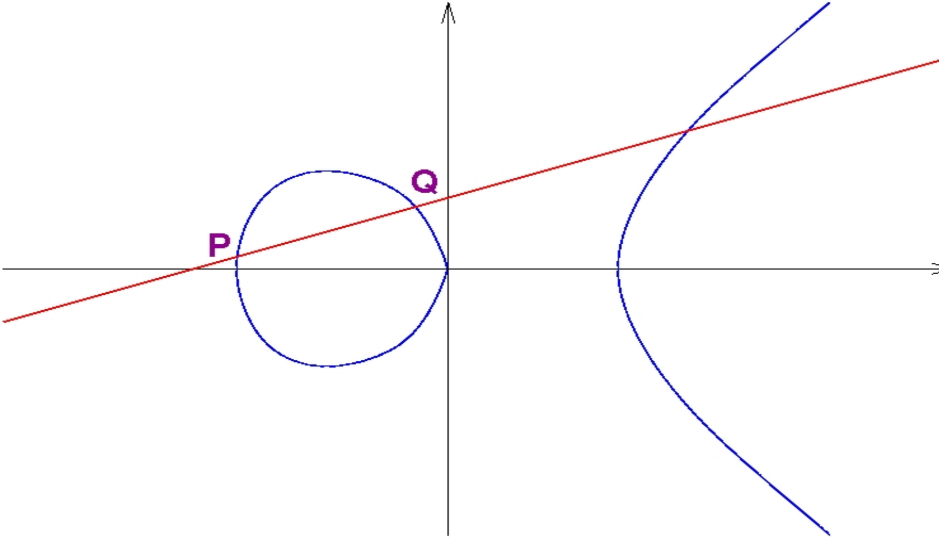
Théorème (Hasse (1936))

$p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$

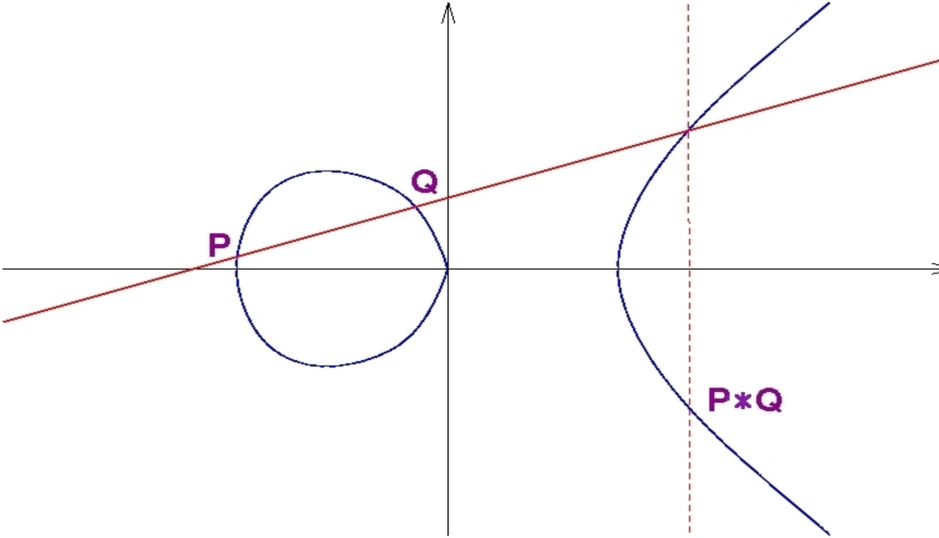
Le groupe des points d'une courbe elliptique



Le groupe des points d'une courbe elliptique



Le groupe des points d'une courbe elliptique



Comment calculer les grandes puissances ?

Dans les protocoles cryptographiques, nous devons calculer de grandes puissances.

Exemple (Curve25519, Dan J. Bernstein (2005))

E_{25519} est la courbe elliptique d'équation $y^2 = x^3 + 486662x^2 + x$ sur $\mathbb{Z}_p$ avec $p = 2^{255} - 19$. Elle a $|E(\mathbb{Z}_p)| \sim 2^{255}$.

Comment calculer les grandes puissances ?

Dans les protocoles cryptographiques, nous devons calculer de grandes puissances.

Exemple (Curve25519, Dan J. Bernstein (2005))

E_{25519} est la courbe elliptique d'équation $y^2 = x^3 + 486662x^2 + x$ sur $\mathbb{Z}_p$ avec $p = 2^{255} - 19$. Elle a $|E(\mathbb{Z}_p)| \sim 2^{255}$.

Soit ℓ un nombre aléatoire, $0 \leq \ell \leq |E(\mathbb{Z}_p)|$. Alors $\ell \geq \frac{|E(\mathbb{Z}_p)|}{2} \sim 2^{254}$ avec probabilité $1/2$. Soit $P \in E(\mathbb{Z}_p)$.

Question

Comment calculons-nous P^ℓ ?

Comment calculer les grandes puissances ?

Dans les protocoles cryptographiques, nous devons calculer de grandes puissances.

Exemple (Curve25519, Dan J. Bernstein (2005))

E_{25519} est la courbe elliptique d'équation $y^2 = x^3 + 486662x^2 + x$ sur $\mathbb{Z}_p$ avec $p = 2^{255} - 19$. Elle a $|E(\mathbb{Z}_p)| \sim 2^{255}$.

Soit ℓ un nombre aléatoire, $0 \leq \ell \leq |E(\mathbb{Z}_p)|$. Alors $\ell \geq \frac{|E(\mathbb{Z}_p)|}{2} \sim 2^{254}$ avec probabilité $1/2$. Soit $P \in E(\mathbb{Z}_p)$.

Question

Comment calculons-nous P^ℓ ?

Exemple

Si on calcule P^ℓ comme $\underbrace{P * P * \cdots * P}_{\ell \text{ fois}}$ on fait $\ell - 1$ multiplications.

Exponentiation rapide

Exemples :

- $P^8 = ((P^2)^2)^2 \rightsquigarrow$ 3 multipl. (en lieu de 7)
- $P^9 = ((P^2)^2)^2 * P \rightsquigarrow$ 4 multipl. (en lieu de 8)
- $P^{10} = (P^5)^2 = (P^4 * P)^2 = ((P^2)^2 * P)^2 \rightsquigarrow$ 4 multipl. (en lieu de 9)

Exponentiation rapide

Exemples :

- $P^8 = ((P^2)^2)^2 \rightsquigarrow$ 3 multipl. (en lieu de 7)
- $P^9 = ((P^2)^2)^2 * P \rightsquigarrow$ 4 multipl. (en lieu de 8)
- $P^{10} = (P^5)^2 = (P^4 * P)^2 = ((P^2)^2 * P)^2 \rightsquigarrow$ 4 multipl. (en lieu de 9)

Remarque : En écrivant les exposants dans la base deux, on obtient :

- $8 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 0 * 2^0$
- $9 = 8 + 1 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0$
- $10 = 8 + 2 = 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0$

Exponentiation rapide

Exemples :

- $P^8 = ((P^2)^2)^2 \rightsquigarrow$ 3 multipl. (en lieu de 7)
- $P^9 = ((P^2)^2)^2 * P \rightsquigarrow$ 4 multipl. (en lieu de 8)
- $P^{10} = (P^5)^2 = (P^4 * P)^2 = ((P^2)^2 * P)^2 \rightsquigarrow$ 4 multipl. (en lieu de 9)

Remarque : En écrivant les exposants dans la base deux, on obtient :

- $8 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 0 * 2^0$
- $9 = 8 + 1 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0$
- $10 = 8 + 2 = 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0$

Théorème

Soit $\ell = \ell_k * 2^k + \ell_{k-1} * 2^{k-1} + \ldots + \ell_1 * 2^1 + \ell_0 * 2^0$. Alors on peut calculer

$$P^\ell = (\cdots((P^2 * P^{\ell_{k-1}})^2 * P^{\ell_{k-2}})^2 * \cdots)^2 * P^{\ell_0}$$

avec au plus $2k = 2\lfloor \log_2 \ell \rfloor$ multiplications (en lieu de $\ell - 1$).

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte :
  $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte :
  $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique des courbes elliptiques :

- recommandation de NSA, standard de NIST

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte : $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique des courbes elliptiques :

- recommandation de NSA, standard de NIST
- SSL/TLS, Chrome, Firefox, Internet Explorer, Opera, Safari, Seamonkey

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte : $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique des courbes elliptiques :

- recommandation de NSA, standard de NIST
- SSL/TLS, Chrome, Firefox, Internet Explorer, Opera, Safari, Seamonkey
- OpenSSH, Tor, Google forward secrecy

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte :
  $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique des courbes elliptiques :

- recommandation de NSA, standard de NIST
- SSL/TLS, Chrome, Firefox, Internet Explorer, Opera, Safari, Seamonkey
- OpenSSH, Tor, Google forward secrecy
- Wii, Bitcoin, cartes d'identité autrichiennes, iOS pour natel, etc.

Exemples d'utilisation pratique de la cryptographie par courbes elliptiques

Pourquoi les courbes elliptiques ?

- les points ont une représentation compacte : $P = (a, b) \in E(\mathbb{Z}_p) \leftrightarrow a \in \mathbb{Z}_p + 1$ bit pour déterminer $b \in \{\pm\sqrt{f(a)}\}$,
- l'opération de groupe peut être calculée efficacement,
- le PLD est le plus difficile possible.

Exemples d'utilisation pratique des courbes elliptiques :

- recommandation de NSA, standard de NIST
- SSL/TLS, Chrome, Firefox, Internet Explorer, Opera, Safari, Seamonkey
- OpenSSH, Tor, Google forward secrecy
- Wii, Bitcoin, cartes d'identité autrichiennes, iOS pour natel, etc.
- WhatsApp, Signal, Threema

Le problème du logarithme discret dans $E(\mathbb{Z}_p)$

Problème du logarithme discret (PLD) (courbe elliptique)

Soit E une courbe elliptique sur $\mathbb{Z}_p$, $P, Q \in E(\mathbb{Z}_p)$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

Le problème du logarithme discret dans $E(\mathbb{Z}_p)$

Problème du logarithme discret (PLD) (courbe elliptique)

Soit E une courbe elliptique sur $\mathbb{Z}_p$, $P, Q \in E(\mathbb{Z}_p)$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

- L'algorithme rho de Pollard est l'algorithme connue le plus efficace pour calculer un logarithme discret dans $E(\mathbb{Z}_p)$ et a complexité $\mathcal{O}(\sqrt{p})$ pour un group d'environ p éléments.

Le problème du logarithme discret dans $E(\mathbb{Z}_p)$

Problème du logarithme discret (PLD) (courbe elliptique)

Soit E une courbe elliptique sur $\mathbb{Z}_p$, $P, Q \in E(\mathbb{Z}_p)$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

- L'algorithme rho de Pollard est l'algorithme connue le plus efficace pour calculer un logarithme discret dans $E(\mathbb{Z}_p)$ et a complexité $\mathcal{O}(\sqrt{p})$ pour un group d'environ p éléments.
- Comme cette algorithme marche sur une groupe quelconque, le PLD dans le groupe des points d'une courbe elliptique est le plus difficile possible.

Le problème du logarithme discret dans $E(\mathbb{Z}_p)$

Problème du logarithme discret (PLD) (courbe elliptique)

Soit E une courbe elliptique sur $\mathbb{Z}_p$, $P, Q \in E(\mathbb{Z}_p)$.
Trouver $\ell \in \mathbb{Z}$ t.q. $P^\ell = Q$, en supposant que ℓ existe.

- L'algorithme rho de Pollard est l'algorithme connue le plus efficace pour calculer un logarithme discret dans $E(\mathbb{Z}_p)$ et a complexité $\mathcal{O}(\sqrt{p})$ pour un group d'environ p éléments.
- Comme cette algorithme marche sur une groupe quelconque, le PLD dans le groupe des points d'une courbe elliptique est le plus difficile possible.
- On a aussi des courbes faibles, pour lesquelles le PLD n'est pas aussi difficile que dans le cas général.

Le PLD est vraiment difficile !

On suppose que pour resoudre le problème du logarithme discret dans un group d'environ p éléments on deut faire environ $\sqrt{p}$ opérations.

Le PLD est vraiment difficile !

On suppose que pour resoudre le problème du logarithme discret dans un group d'environ p éléments on deut faire environ $\sqrt{p}$ opérations. Alors, pour résoudre un problème du logarithme discret dans un groupe d'environ 2^{255} éléments (p.e. la courbe 25519), nous avons besoin de faire 2^{128} operations, ce qui prend environ $1.02 * 10^{18}$ années.

Le PLD est vraiment difficile !

On suppose que pour resoudre le problème du logarithme discret dans un group d'environ p éléments on deut faire environ $\sqrt{p}$ opérations. Alors, pour résoudre un problème du logarithme discret dans un groupe d'environ 2^{255} éléments (p.e. la courbe 25519), nous avons besoin de faire 2^{128} operations, ce qui prend environ $1.02 * 10^{18}$ années. Comparer avec l'âge de la terre de $4.5 * 10^{9}$ années.

Le PLD est vraiment difficile !

On suppose que pour resoudre le problème du logarithme discret dans un group d'environ p éléments on deut faire environ $\sqrt{p}$ opérations. Alors, pour résoudre un problème du logarithme discret dans un groupe d'environ 2^{255} éléments (p.e. la courbe 25519), nous avons besoin de faire 2^{128} operations, ce qui prend environ $1.02 * 10^{18}$ années. Comparer avec l'âge de la terre de $4.5 * 10^9$ années.

Merci pour votre attention !

Références

- analyse frequentiélle `http://www.dcode.fr/analyse-frequences`
- chiffre de Vigenère `http://www.dcode.fr/chiffre-vigenere`
- `http://www.cryptage.org`
- Douglas Stinson, "Cryptographie : Théorie et pratique"
- Lawrence Washington, "Elliptic curves : number theory and cryptography"