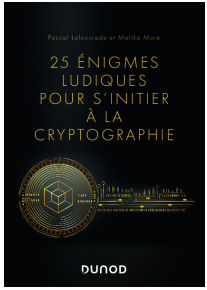
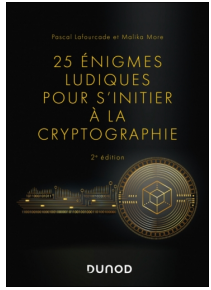
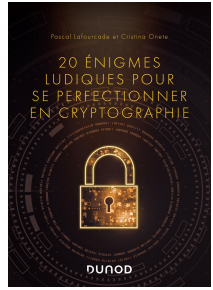
Cryptographie & Pédagogie







Pascal Lafourcade

LIMOS — UNIVERSITÉ Clermont Auvergne — IREM Clermont-Ferrand

Le jeu au service des chiffres

Didapro mars 2026, Grenoble

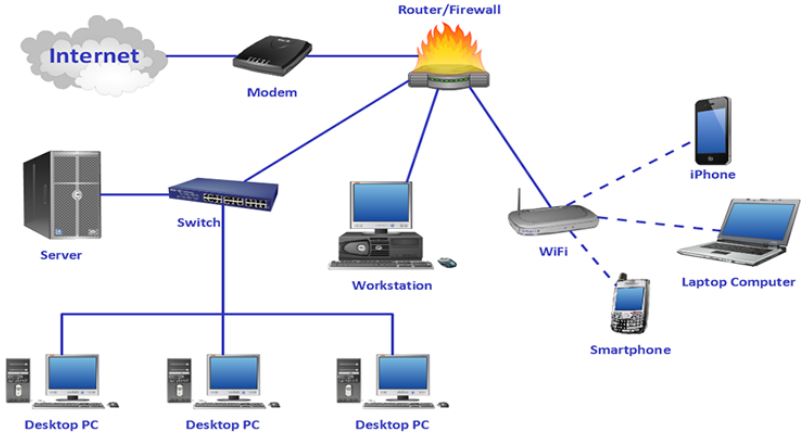

https://www.


carte d'assurance maladie
vitale

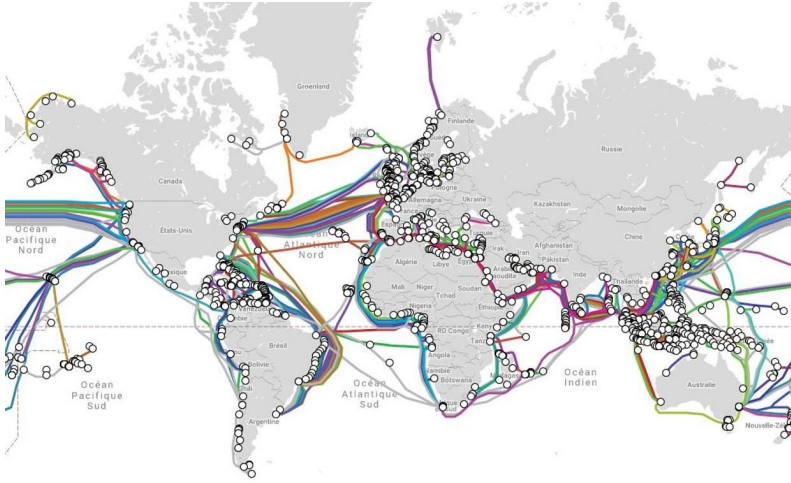

VISA
VISA


BANQUE

Une réalité physique



Cables



https://www.submarinecablemap.com/

Plan

Plan

Stéganographie : - 500

Histoires d'Hérodote (- 445)

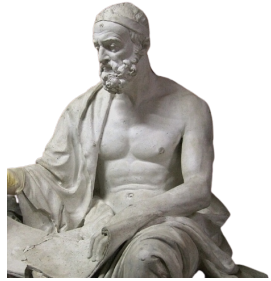
- Tablette de cire
- Tatouage d'esclaves

Atelier

Plutarque raconte son utilisation par Lysandre de Sparte

Carré de Polybe : - 150

Atelier



	1	2	3	4	5
1	P	O	L	Y	B
2	E	M	A	U	D
3	I/J	T	C	F	G
4	H	K	N	Q	R
5	S	V	W	X	Z

Atelier

AVE CESAR
DYH FHVDU

Vigenère : 1586

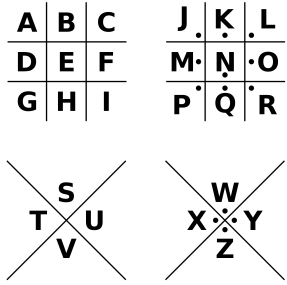
Atelier

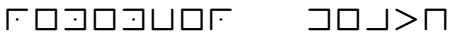
Blaise de Vigenère, né en 1523 à Saint-Pourçain-sur-Sioule

B	L	A	I	S	E
1	3	2	1	3	2
C	O	C	J	V	G

Atelier

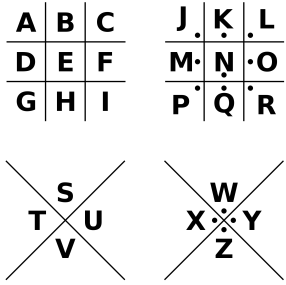
Cimetière Trinity Church, NewYork 1697

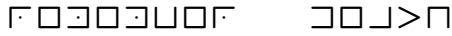




Atelier

Cimetière Trinity Church, NewYork 1697





REMEMBER DEATH

Principes de Kerchoff

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

"*La sécurité d'un système cryptographique doit totalement dépendre du secret de la clé et non du secret de l'algorithme.*"

La cryptographie du primaire à l'Université

Primaire, Collège, Lycée

Missions Cryptographiques :

- MathC2+ en 2nde
- Fête de la science (2nde, 1ère, BTS)
- Gagnants auvergnats concours Alkindi
- Atelier APMEP
- Salon Culture & Jeux Mathématiques en 2020
- RJMI à Clermont en 2020

Université

- BUT 2A : **Cryptographie**
- BUT 3A : **Cours Sécurité**
- M1 Introduction à la **cryptographie post-quantique**
- M2 Sécurité des systèmes d'information : **Sécurité des systèmes d'information**

Mission Cryptographie Disponible 24h/24h et 7j/7j

Initiation à la cryptographie

- Résoudre des challenges
- Activité ludique
- 1 concept = 1 challenge = 1 lettre

https ://sancy.iut.uca.fr/~lafourcade/mission-crypto.html

Aide à la conception

Atelier : un site pour créer des missions cryptographiques

https://mission-crypto.limos.fr

Atelier

Classer ces 15 mots de passe en deux catégories : les forts et les faibles ?

```
pwd 1  : 12345678
pwd 2  : Azerty12345
pwd 3  : 7hY3^b
pwd 4  : 7Vy^$FvRw6)5
pwd 5  : m}87h@
pwd 6  : 1aqw2zsx
pwd 7  : 1q2w3e4r5t
pwd 8  : V6rr3!BXY59ru3U
pwd 9  : KaNgOuRoU
pwd 10 : password
pwd 11 : T8j9j8U!dws5rz699t849
pwd 12 : 987654321
pwd 13 : 6O!LoFkudk*15
pwd 14 : Zb2^
pwd 15 : iloveyou
```

Solution

11 FAIBLES :

```
pwd 1  : 12345678
pwd 2  : Azerty12345
pwd 3  : 7hY3^b
pwd 5  : m}87h@
pwd 6  : 1aqw2zsx
pwd 7  : 1q2w3e4r5t
pwd 9  : KaNgOuRoU
pwd 10 : password
pwd 12 : 987654321
pwd 14 : Zb2^
pwd 15 : iloveyou
```

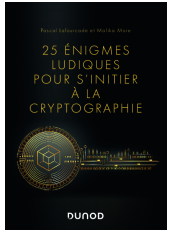
4 FORTS :

```
pwd 4  : 7Vy^$FvRw6)5
pwd 8  : V6rr3!BXY59ru3U
pwd 11 : T8j9j8U!dws5rz699t849
pwd 13 : 6O!LoFkudk*15
```

En réalité

En réalité

Fuites de données ...



On the Privacy Impacts of Publicly Leaked Password Databases, O. Heen, C. Neumann, DIMVA'17

7 conseils pour créer vos mots de passe

Un mot de passe

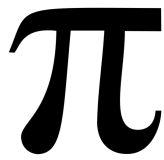
1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il n'est jamais assez sophistiqué
7. la taille compte.

7 conseils pour créer vos mots de passe

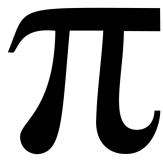
Un mot de passe

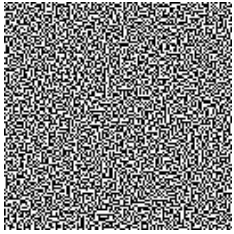
1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il n'est jamais assez sophistiqué
7. la taille compte.

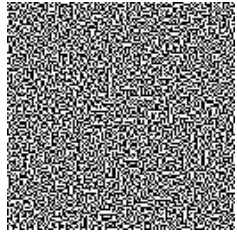
Atelier + Poster Session

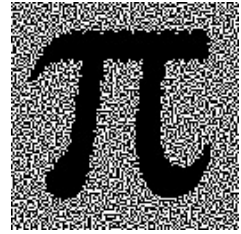


Atelier + Poster Session



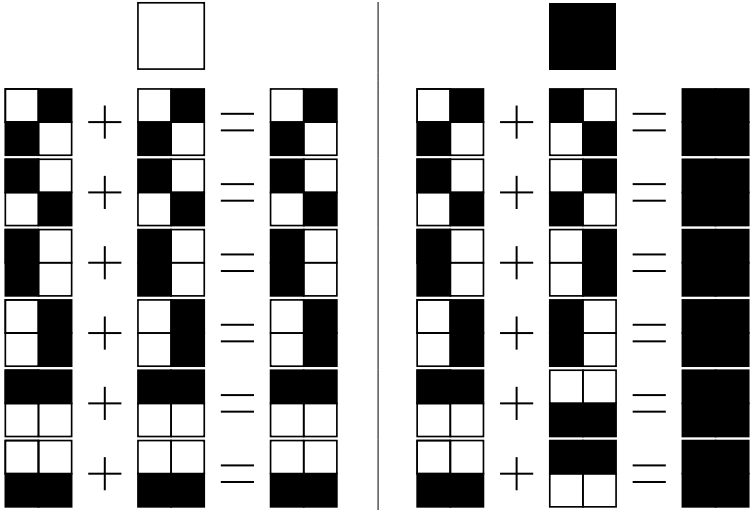






Cryptographie visuelle


M. Naor et A. Shamir, "*Visual Cryptography*", EUROCRYPT 1994



https ://sancy.iut.uca.fr/~lafourcade/Cryptovisuelle/

Plan

À vos papiers et crayons

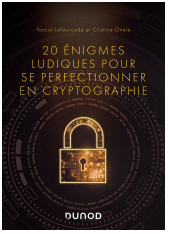
Atelier

Vous avec reçu un papier avec deux couples de nombres

Votre mission

Trouvez mes deux secrets

- à deux pour les points en rouge
- à trois pour les points en bleu

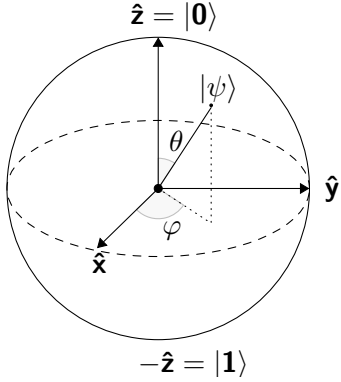


Plan

Qubit dans les années 80 ... Benjamin Schumacher 1995

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ avec } (\alpha, \beta) \in \mathbb{C}, \text{ tel que } \alpha\,|0\rangle + \beta\,|1\rangle = 1$$

$$||\psi||^2 = |\alpha|^2 + |\beta|^2 = \alpha.\overline{\alpha} + \beta.\overline{\beta} = 1$$



Ordinateurs quantiques

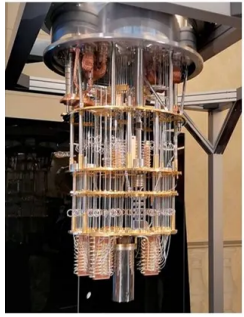
IBM Google rigetti

- 1998 : 2 qbits, IBM
- 1999 : 3 qbits, IBM
- 2001 : 7 qbits, IBM
- 2017 : 50 qbits, IBM Q50
- 2019 : 53 qbits, Google Sycamore
- 2021 : 90 qbits, Rigetti Aspen-9
- 2021 : 127 qbits, IBM Eagle
- 2022 : 433 qbits, IBM Osprey
- Dec 2023 : 1 121 qubits, IBM Condor

D:wave

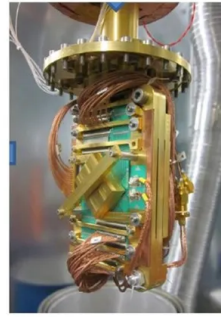
- 2011 : 128 qbits, One
- 2013 : 512 qbits, Two
- 2015 : 1152 qbits, 2X
- 2017 : 2048 qbits, 2000Q
- 2020 : 5760 qbits, Advantage
- 2024 : 7440 qbits, Advantage 2

Ordinateurs quantiques



IBM

rigetti



D:Wave

Portes quantiques

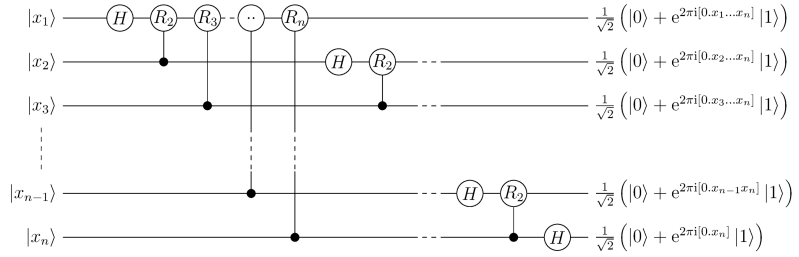
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

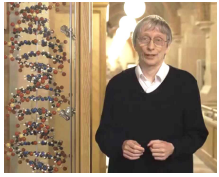
Circuits quantiques



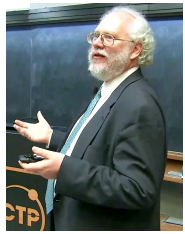
Transformée de Fourrier quantique

Algorithmes quantiques

- Algorithme de Deutsch (1985) et Deutsch-Jozsa (1992)
- Algorithme de Simon (1994)
- Algorithme de Shor (1994)
- Algorithme de Grover (1996)

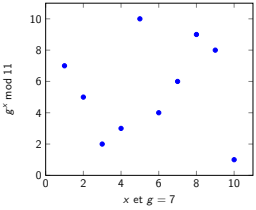



Cryptographie Pré-quantique



Deux problèmes :

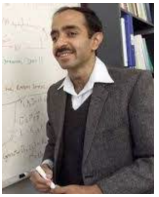
- Factorisation : $n = p \times q$ difficile de trouver p et q.
- Logarithme disctet : $g, p, g^x \bmod p$ difficile de trouver x.



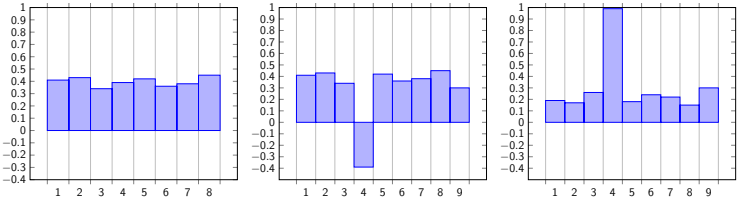
Ces deux problèmes sont cassés par l'algorithmes de **Shor !**

"Store-now, decrypt-later"

Grover 1996



Trouver $x \in \{0,1\}^n$ avec $F(x)$ en $\sqrt{2^n}$ évaluations de F



Oracle quantique qui détermine x

Diminue légèrement la sécurité pour :

- les fonctions de hachages de $O(2^{\frac{N}{2}})$ à $O(2^{\frac{N}{3}})$
- les chiffrements symétriques de $O(2^n)$ à $O(2^{\frac{n}{2}})$

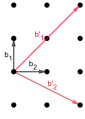
Cryptographie Post-Quantique

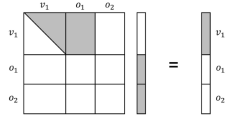
- Fonctionne sur les ordinateurs classiques
- Résite à un ordinateur quantique

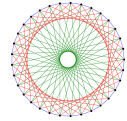
Les problèmes difficiles sous-jacents sont différents !

5 familles de problèmes difficiles

- Fonctions de hachage
- Réseaux Euclidiens (Lattices)
- Codes
- Systèmes Multivariés
- Isogénies





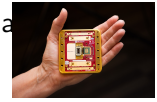


Compétition du NIST lancée en 2017

- 30 novembre 2017 : 69 sousmissions Round 1
- 30 janvier 2019 : 26 sousmissions choisies pour le Round 2
- 22 juillet 2020 : 7+8 sousmissions choisies pour le Round 3
- 5 juillet, 2022 :
  - KEM : Kyber
  - Signature : Dilithium, Falcon, SPHINCS+
- 13 août 2024, NIST publie les standards :
  - FIPS 203 (Kyber),
  - FIPS 204 (Dilithium)
  - FIPS 205 (SPHINCS+)
  - FIPS 206 (FALCON à venir)
- 10 mars 2025, NIST annonce le vainqueur du Round 4 : KEM HQC

Changements en cours

- 2014 : La Fondation Linux a créé la Post-Quantum Cryptography Alliance (PQCA)
- Septembre 2023 : PQXDH protocol (Signal)
- Février 2024 : PQ3 protocol (imessage)
- Avril 2024 : Chrome $>$ 124 utilise Kyber768 pour TLS 1.3
- Mai 2024 : migre vers Kyber pour l'échange de clés TLS.
- Le 7 juin 2024, ont proclamé 2025 comme l'Année Internationale de la Science et de la Technologie Quantiques
- Février 2025 : annonce 1 million de qbits topologiques, Majorana



- Le 10 juin 2025, annonce Quantum Starling pour 2029 !

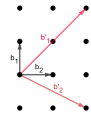
À retenir

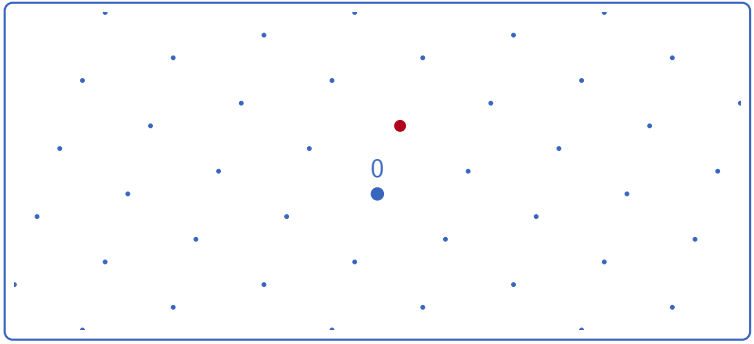
NIST

Novembre 2024

Algorithmes	Transition
ECDSA	Déprécié après 2030
	Interdit après 2035
RSA	Déprécié après 2030
	Interdit après 2035

Problème difficile sur les lattices (SVP)

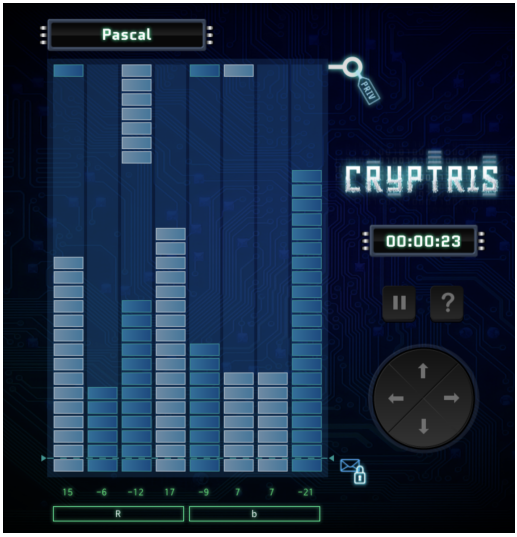


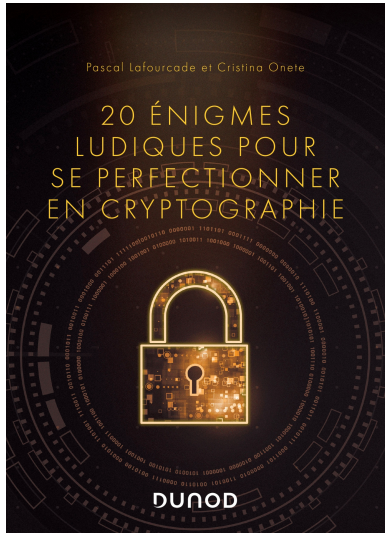


Shortest Vector Problem (SVP) : Trouver un vecteur petit de $\mathcal{L} \setminus \{0\}$.

$||v|| = \sqrt{\sum_{i=i}^{n} v_i^2}$

SVP





https://cryptris.nl/index_fr.html

Activité sur SVP

- Clé secréte : $sk = [\mathbf{s}_1|\mathbf{s}_2] = \begin{pmatrix} 0 & 3 \\ 8 & 0 \end{pmatrix}$, $|\mathbf{s}_1| = 8$, $|\mathbf{s}_2| = 3$, angle $= 90$, et $A = \begin{pmatrix} -8 & -3 \\ -5 & -2 \end{pmatrix}$, $|\det(A)| = 1$
- Clé publique : $pk = [\mathbf{p}_1|\mathbf{p}_2] = sk \cdot A = \begin{pmatrix} -15 & -6 \\ -64 & -24 \end{pmatrix}$, $|\mathbf{p}_1| = 65.73$, $|\mathbf{p}_2| = 24.74$

Chiffrement de $m = (1, 0) \in \{0, 1\}^2$ avec pk

1. Choisir au hasard $(b_1, b_2) = (2, 3)$
2. $c = (1, 0) + b_1 * \mathbf{p}_1 + b_3 * \mathbf{p}_2 = (-47, -200)$

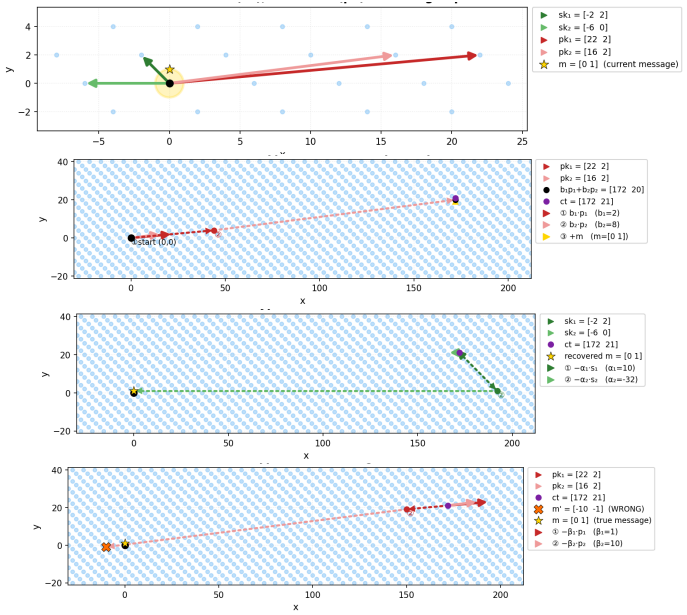
Déchiffrement de c avec sk

1. Supposons que $c = (-47, -200) = \alpha_1\mathbf{s}_1 + \alpha_2\mathbf{s}_2$
2. Résoudre : $\alpha_1 = -25.00$, $\alpha_2 = -15.67$ donc $\alpha_1 = -25$, $\alpha_2 = -16$
3. $m = (-47, -200) - (-25)\mathbf{s}_1 - (-16)\mathbf{s}_2 = (1, 0)$



Goldreich, O., Goldwasser, S., Halevi, S. (CRYPTO 1997)
Public-key cryptosystems from lattice reduction problems

SVP



Plan

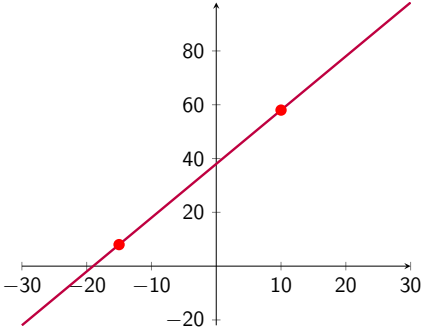
Partage de secret de Shamir 1979

Atelier

Shamir, Adi (1979), "*How to share a secret*", Communications of the ACM.

Méthode

Avec 1 voisin et 2 points rouges, résoudre un système de deux équations.

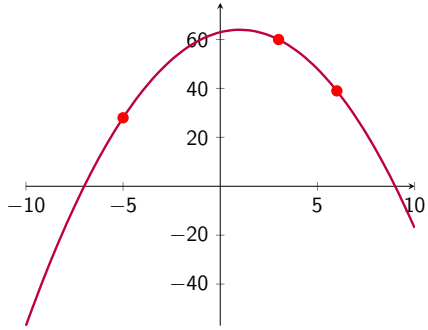


$y = ax + s$ $y = 2x + 38$

https://sancy.iut.uca.fr/~lafourcade/Shamir.html

Atelier

Avec 2 voisins et **3 points bleus**



$y = ax^2 + bx + s$ $\quad$ $y = -x^2 + 2x + 63$

https://sancy.iut.uca.fr/~lafourcade/Shamir.html

Partage de secret de Shamir vérifiable **Atelier**

A practical scheme for non-interactive verifiable secret sharing, P. Feldman, FOCS 1987

Comment détecter les faux points !

- Les points valident vérifient : $y = ax + s$
- Avec p, g, g^a et g^s, on peut savoir si son point est correct.

$$g^y = g^{ax+s} = (g^a)^x * g^s \mod p$$

Remarque : Si $s > p$ et $a > p$ alors il exsite $a' < p$ et $s' < p$ tels que $g^a = g^{a'} \mod p$ et $g^s = g^{s'} \mod p$, ainsi il suffit de vérifier $y = a'x + s' \mod p - 1$

• Pour les points rouges avec $g = 2$, $p = 11$ et $g^a = 4$ et $g^s = 3$

$$2^y = 4^x * 3 = 2^{2x} * 2^8 \mod 11 \qquad \text{ou} \qquad y = 2x + 8 \mod 10$$

$A = (2, 42)$: $2^{42} = 4 = 4^2 * 3 \mod 11$ ou $42 = 2 = 2 * 2 + 8 \mod 10$

$\mathbf{B} = (\mathbf{4}, \mathbf{45})$: $2^{45} = 10 \neq 9 = 4^4 * 3 \mod 11$ ou $45 = 5 \neq 6 = 2 * 4 + 8 \mod 10$

Pour les points bleus !

$$g^y = g^{ax^2+bx+s} = (g^a)^{x^2} * (g^b)^x * g^s \mod p$$

- Pour les points rouges avec $g = 2$, $p = 11$ et $g^a = 6$, $g^b = 4$ et $g^s = 3$

$2^y = 6^{x^2} * 4^x * 8 = 2^{9x^2} * 2^{2x} * 2^3 \mod 11$ ou $y = 9x^2 + 2x + 3 \mod 10$

$A = (6, 39)$: $2^{39} = 6 = 6^{6^2} * 4^6 * 8 \mod 11$ ou $39 = 9 = 9 * 6^2 + 2 * 6 + 8 \mod 10$
$\mathbf{B} = (\mathbf{2}, \mathbf{56})$: $2^{56} = 9 \neq 8 = 6^{2^2} * 4^2 * 8 \mod 11$ ou $56 = 6 \neq 3 = 9 * 2^2 + 2 * 2 + 3 \mod 10$

Plan

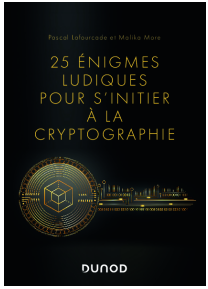
Conclusion

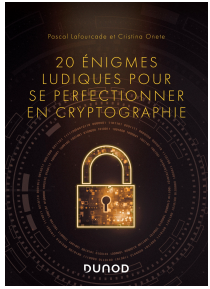
- La cryptographie est omniprésente
- Impossible de faire illusion
- Il faut éduquer le plus tôt possible !

Conclusion

ISO

- Apprendre en s'amusant
- Travail en équipe
- Étudiants actifs
- Découverte ... imagination





Questions ?

pascal.lafourcade@uca.fr

https://mission-crypto.limos.fr

Atelier (A2) Un site pour créer des missions cryptographiques
Mercredi 11h - 12h

Poster : Cinq activités sur les images numériques