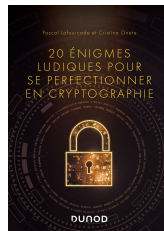


Cryptographie & Pédagogie



Pascal Lafourcade

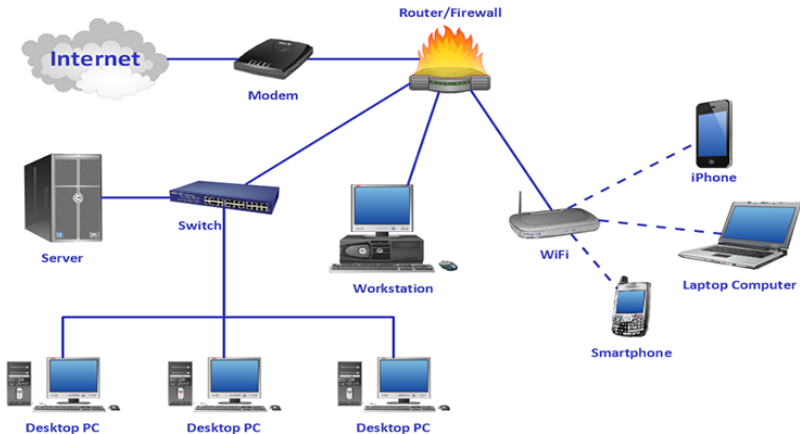


Le jeu au service des chiffres

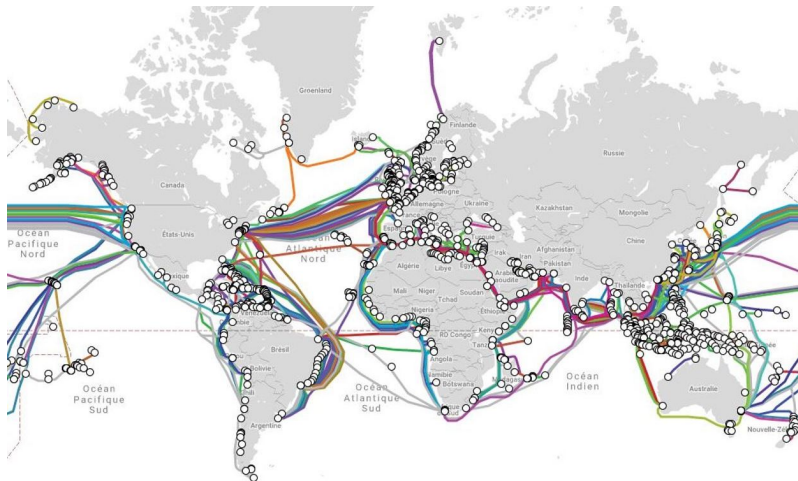
Didapro mars 2026, Grenoble



Une réalité physique



Cables



<https://www.submarinecablemap.com/>

Plan

Cryptographie sans ordinateur

Activité

Cryptographie post-quantique

Activité le retour

Conclusion

Stéganographie : 500 av J.-C

Histoires d'Hérodote (445 av J.-C)



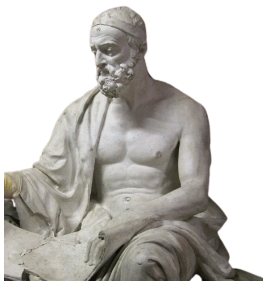
- ▶ Tablette de cire
- ▶ Tatouage d'esclaves

Scytale : 404 av. J.-C



Plutarque raconte son utilisation par Lysandre de Sparte

Carré de Polybe : 150 av. J.-C.



	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

César : 1er siècle av. J.-C.



AVE CESAR
DYH FHVDU

Vigenère : 1586



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

PigPen : XVIème siècle

Cimetière Trinity Church, NewYork 1697



□ ◻ ◻ ◻ ◻ ◻ ◻ ◻

A	B	C
D	E	F
G	H	I

J.	K.	L.
M.	N.	O.
P.	Q.	R.

~~S
T U
V~~

~~$$\begin{array}{c} W \\ X : Y \\ Z \end{array}$$~~
$$\square \square \neg \square$$

PigPen : XVIème siècle

Cimetière Trinity Church, New York 1697



REMEMBER

DEATH

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		

Principes de Kerchoff : 1883

“La Cryptographie Militaire”



JOURNAL
DES
SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire
précieux 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**



Initiation à la cryptographie

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



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

<https://mission-crypto.limos.fr>

Atelier : un site pour créer des missions cryptographiques

Hygiène numérique

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 : 60!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  : 60!LoFkudk*15
```



En réalité



En réalité



Fuites de données ...

rockyou

New RockYou Password

Retype Password

☒ I agree to the [Terms of Service](#).

Year of Birth

Sex

Country

None

Zip/Postal

Submit

Back

```
79985232-|--| a@fbi.gov-|-+ujc1L90fBnioxG6CatHBw==|-anniversary|--|
105089730-|--| gon@ic.fbi.gov-|-9nCgb38RHIw==|-band|--|
108684532-|--| burn@ic.fbi.gov-|-EQ7fIpT7i/Q=-|-numbers|--|
53041670-|--| w-|-hRwtmq98mKzioG6CatHBw==|-|--|
94038395-|--| n@ic.fbi.gov-|-MreVpEovY17ioxG6CatHBw==|-eod date|--|
116097938-|--| -|-Tur7wt2zH5CwIIHfjvcHKQ==|-SH?|--|
83310434-|--| c.fbi.gov-|-NLupdfyYrsM=-|-ATP_MIDDLE|--|
113389790-|--| w-|-iMhaearHXjPioxG6CatHBw==|-w|--|
113931981-|--| @ic.fbi.gov-|-lTnosXxYnP3ioxG6CatHBw==|-See MSDN|--|
114081741-|--| lom@ic.fbi.gov-|-ZcDbLlvCad0=-|-fuzzy boy 20|--|
106145242-|--| @ic.fbi.gov-|-xc2KumNGzYfioxG6CatHBw==|-4s|--|
106437837-|--| i.gov-|-adIewKvmJEsFqx0HfOfRxxg=-|-|--|
96649467-|--| ius@ic.fbi.gov-|-lsYw5KRKNT/ioxG6CatHBw==|-glass of|--|
96670195-|--| .fbi.gov-|-X4+k4uhy0h/ioxG6CatHBw==|-|--|
105095956-|--| warthlink.net-|-ZU2tTTFIZq/ioxG6CatHBw==|-socialsecurity#|--|
108260815-|--| r@genext.net-|-MuKnZ7KtsiHioxG6CatHBw==|-socialsecurity|--|
83508352-|--| h @hotmail.com-|-ADEcoaN2oUM=-|-socialsecurityno.|--|
83023162-|--| k 59@aol.com-|-9HT+kVHQfs4=-|-socialsecurity name|--|
88331688-|--| b .edu-|-nNiwEcoZT8mXrIXpAZiRHQ=-|-ssn#|--|
```



Olivier Heen, Christoph Neumann “On the Privacy Impacts of Publicly Leaked Password Databases” DIMVA 2017.

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.



Tour de magie



Un spectateur choisit un tableau de bits

0	1	0	0	1
1	1	1	1	1
1	0	0	0	0
0	1	1	0	0
0	0	1	1	1

0	1	0	0	1	0
1	1	1	1	1	1
1	0	0	0	0	1
0	1	1	0	0	0
0	0	1	1	1	1
0	1	1	0	1	1

Le magicien ajoute les bits en vert.

Tour de magie



Le magicien se tourne et le spectateur modifie un bit.

Le magicien se retourne et trouve le bit modifié.

0	1	0	0	1	0
1	1	1	0	1	1
1	0	0	0	0	1
0	1	1	0	0	0
0	0	1	1	1	1
0	1	1	0	1	1

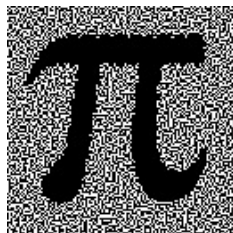
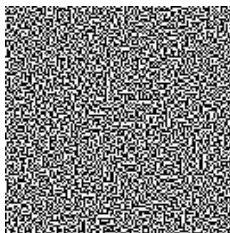
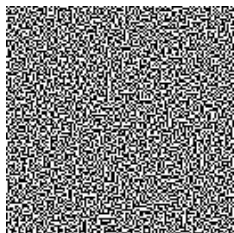
Comment fait-il ?

<https://sancy.iut.uca.fr/~iso/>

Théorie des codes - 3e éd 2018, Jean-Guillaume Dumas, Jean-Louis Roch, Sébastien Varrette, Eric Tannier.

π

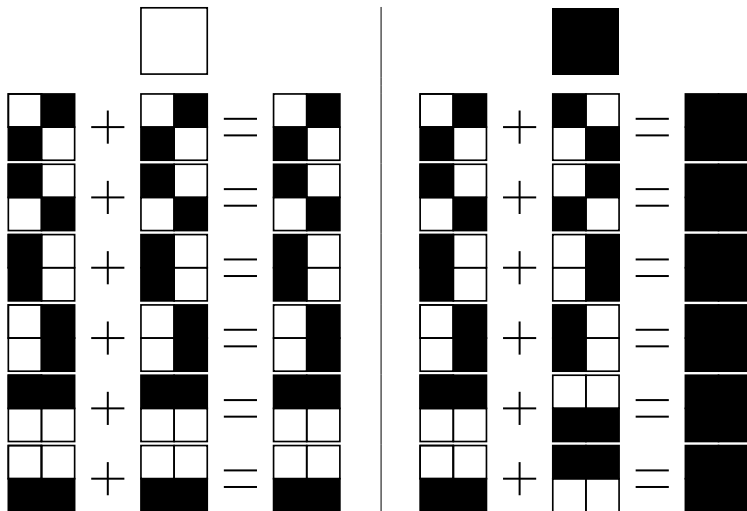
π



Cryptographie visuelle



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



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

Plan

Cryptographie sans ordinateur

Activité

Cryptographie post-quantique

Activité le retour

Conclusion

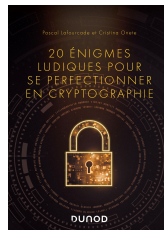
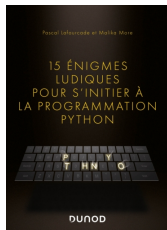
À vos papiers et crayons

Vous avez 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

Cryptographie sans ordinateur

Activité

Cryptographie post-quantique

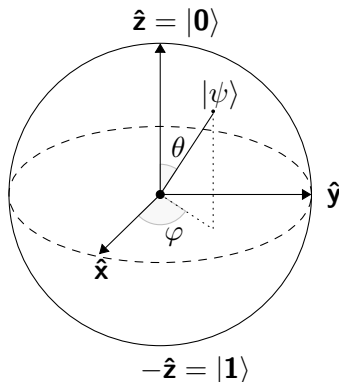
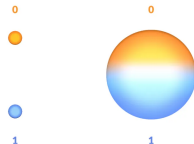
Activité le retour

Conclusion

Qubit dans les années 80 ... Benjamin Schumacher 1995

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

$$||\psi||^2 = |\alpha|^2 + |\beta|^2 = \alpha \cdot \bar{\alpha} + \beta \cdot \bar{\beta} = 1$$



Ordinateurs quantiques

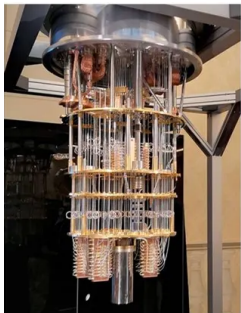


- ▶ 1998 : 2 qbits, IBM
- ▶ 1999 : 3 qbits, IBM
- ▶ 2001 : 7 qbits, IBM
- ▶ 2017 : 50 qbits, IBM Q50
- ▶ 2019 : 53 qbits, Google Sycamore
- ▶ 2021 : 90 qbits, Rigetti Aspen-9
- ▶ 2021 : 127 qbits, IBM Eagle
- ▶ 2022 : 433 qbits, IBM Osprey
- ▶ Dec 2023 : 1 121 qubits, IBM Condor



- ▶ 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

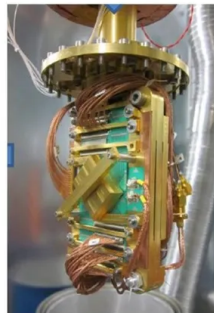
Ordinateurs quantiques



IBM



rigetti



D:wave

Portes quantiques

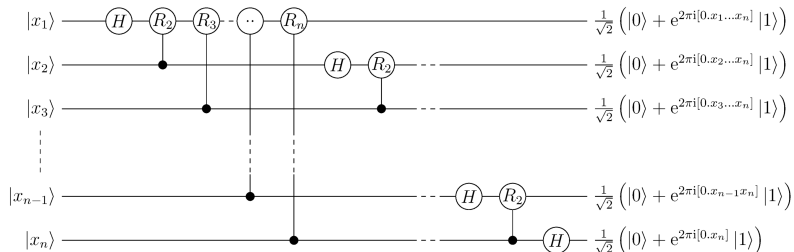
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

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

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

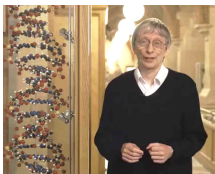
Circuits quantiques



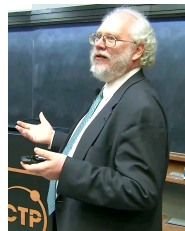
Transformée de Fourier quantique

Algorithmes quantiques

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

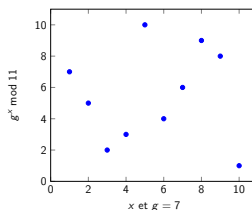


Cryptographie Pré-quantique



Deux problèmes :

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

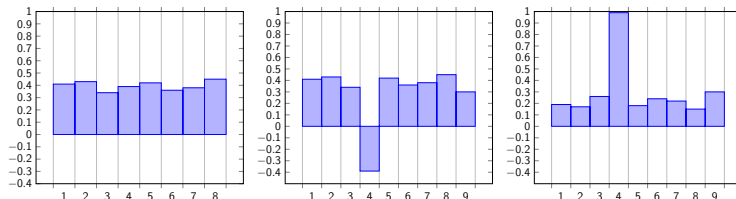


Ces deux problèmes sont cassés par l'algorithmes de **Shor** !

“Store-now, decrypt-later”



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



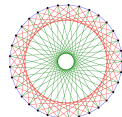
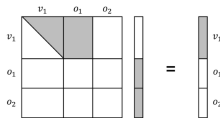
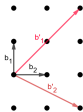
- ▶ Fonctionne sur les ordinateurs classiques
- ▶ Résiste à un ordinateur quantique



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

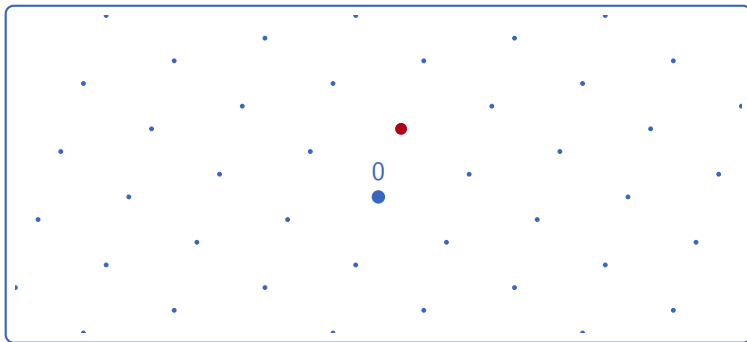
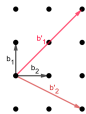
- ▶ 2014 : La Fondation Linux a créé la Post-Quantum Cryptography Alliance (PQCA)
- ▶ Septembre 2023 : PQXDH protocol (Signal) 
- ▶ Février 2024 : PQ3 protocol (imessage) 
- ▶ Avril 2024 :  Chrome > 124 utilise Kyber768 pour TLS 1.3
- ▶ Mai 2024 :  migre vers Kyber pour l'échange de clés TLS.
- ▶ Le 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 !



Novembre 2024

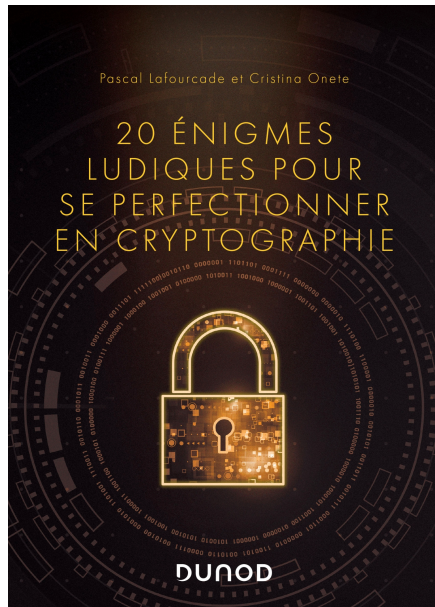
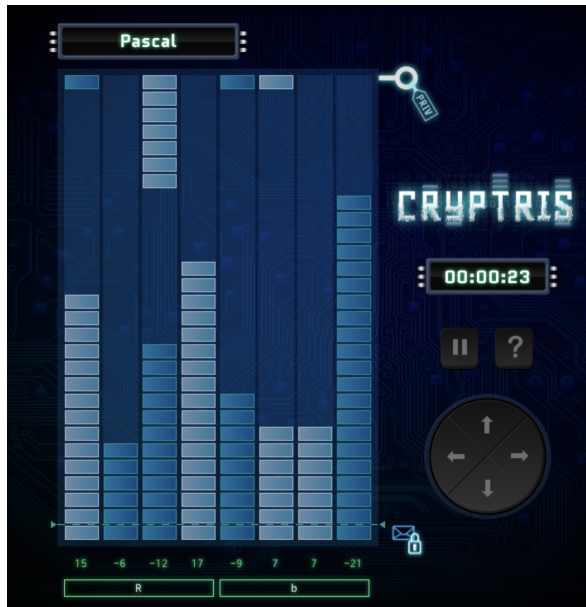
Algorithmes	Transition
ECDSA	Déprécié après 2030
	Interdit après 2035
RSA	Déprécié après 2030
	Interdit après 2035

Problème difficile sur les lattices (SVP)



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

$$\|v\| = \sqrt{\sum_{i=1}^n v_i^2}$$



Plan

Cryptographie sans ordinateur

Activité

Cryptographie post-quantique

Activité le retour

Conclusion

Partage de secret de Shamir 1979

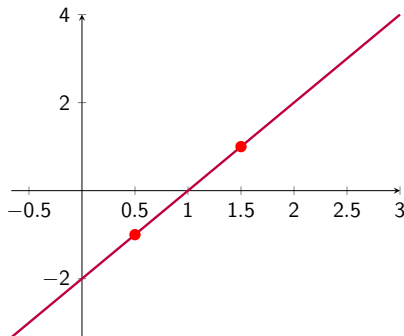


Shamir, Adi (1979), "How to share a secret", Communications of the ACM.

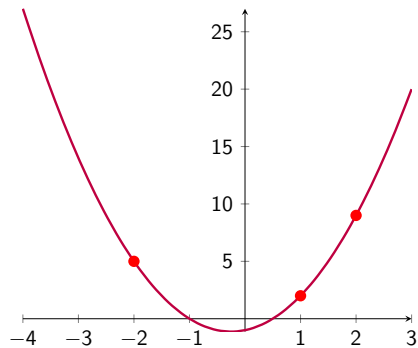
Méthode

Avec les 2 points des lettres précédentes.

Résoudre un système de deux équations.



Shamir le retour



$$y = ax^2 + bx + s$$

Partage de secret de Shamir vérifiable

Feldman, Paul (1987). "A practical scheme for non-interactive verifiable secret sharing". Symposium on Foundations of Computer Science 1987.

Comment détecter les faux points !

- ▶ Les points valides 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 existe $a' < p$ 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 $g^s = 3$

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

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

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

Partage de secret de Shamir vérifiable

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 $g^s = 3$

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

$$A = (6, 39) : 2^{39} = 6 = 6^{6^2} * 4^6 * 8 \mod 11 \text{ ou } 39 = 9 = 9 * 6^2 + 2 * 6 + 8 \mod 10$$

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

Plan

Cryptographie sans ordinateur

Activité

Cryptographie post-quantique

Activité le retour

Conclusion

Conclusion

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

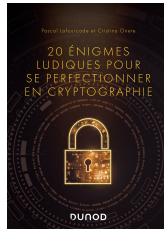


Conclusion



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





Questions ?

pascal.lafourcade@uca.fr

<https://mission-crypto.limos.fr>