ICS - Information Security Systems
Lecture 1: Introduction to Cryptography

2025-2026

What are your expectations for this course?

What are your expectations for this course?

Week 1: Introduction to cybersecurity

Week 2: Public Key Cryptography

Week 3: Symmetric Cryptography

Week 4: Main ATTACKS (Presentations)

Week 5: PKI, TLS, Malwares

Week 6: TOR, ZKP, Bitcoin

What is Cryptography?

- **Goal**: protect secret data against adversaries
  - Authenticated communications (email, web, card payments, ...)
  - Storage (encrypted disk, ...)
  - Computations (electronic voting, ...)
  - ...
- **Use on different hardware**:
  - High-end processors, mobile phones, microcontrollers, dedicated hardware
  - Varying constraints: throughput & latency, code/circuit size, energy consumption, ...
- **Doing crypto**:
  - Designing new primitives, constructions, protocols, ...
  - Analysing existing primitives, ...
  - Deploying crypto in products (implementations, optimisation, integration)

What is this course about?

- **Basic concepts of cryptography**: adversary model, security definition, ...
- **Cryptographic constructions**: block ciphers, key exchange, ...
- **Some standard attacks**: birthday attack, ...
- **Practical usage**: what's inside TLS?
- **Post-quantum**: new standards?

But not (really) about:

- Implementation and design of standard cryptographic libraries

Goal: to answer YOUR questions during the course.

Why Secure Our Digital Use?

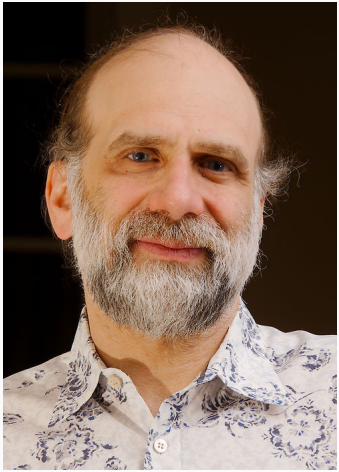
Why Secure Our Digital Use?

- Digital tools are everywhere, but security is often overlooked.
- Main risks:
  - Theft or loss of sensitive data and devices.
  - Disruption of industrial systems (power, water...).
- Impact: financial loss, operational downtime, reputational damage.
- Mitigation:
  - Simple, low-cost good practices.
  - Employee awareness and training.

In 2023

- 6 months to detect a data breach.
- 43% of cyberattacks target small businesses.
- 91% of attacks are launched through a phishing email.
- A company falls victim to a ransomware attack every 14 seconds.
- 38% of malicious attachments are disguised as Microsoft Office or similar files.
- Companies faced an average of 22 security breaches in 2020.
- The global cost of cybercrime will reach $10.5 trillion per year by 2025.
- Estimates show that the cybersecurity market will reach $300 billion by 2024.
- A 400% increase in cyberattacks in France since 2020.

“Security is a process, not a product.”, Bruce Schneier



Standardisation Institutes

- France: ANSSI
- United States: NIST / NSA
- Germany: BSI
- United Kingdom: NCSC

Refer to them for any research on cryptography/security:

The ANSSI website ”aims to answer your cybersecurity questions and share with you targeted and accessible information.”[1]

[1] source: `https://www.ssi.gouv.fr/`

Références

LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS - MÉTHODE DE CLASSIFICATION: cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

La méthode EBIOS Risk Manager : https://cyber.gouv.fr/la-methode-ebios-risk-manager

Recommandations pour la protection des systèmes d'information essentiels : https://cyber.gouv.fr/publications/recommandations-pour-la-protection-des-systemes-dinformation-esse

... Many others !!

Références

Guide d'hygiène informatique :

`cyber.gouv.fr/publications/guide-dhygiene-informatique`

14 Key Actions for Digital Security (1/2)

1. Choose strong, unique passwords.
2. Keep software up to date.
3. Know your users and service providers.
4. Make regular backups.
5. Secure your company Wi-Fi.
6. Treat smartphones and tablets like computers.
7. Protect data when travelling.
8. Be careful with email use.

14 Key Actions for Digital Security (2/2)

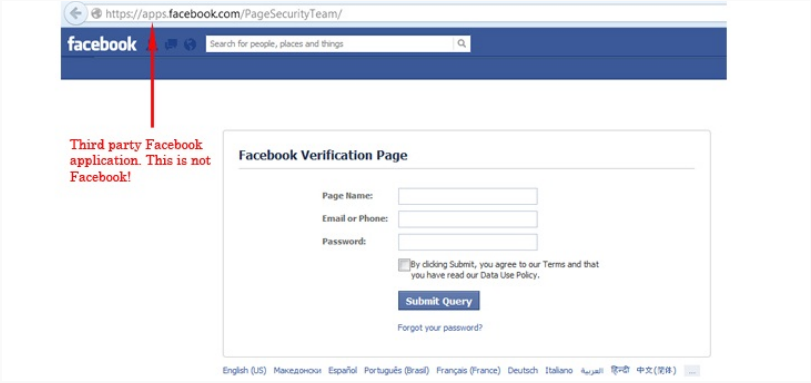
9. Download software only from official sources.
10. Stay vigilant when paying online.
11. Separate personal and professional uses.
12. Protect personal, professional and digital identity data.

Cyberattacks

5 Familles de Cybercriminalité

- Fraud
- Sabotage
- Ransomware
- Espionage
- Destabilization

Escroquerie : Phishing



Voyant + Papillon

In 2019

CLASSEMENT VADESECURE DES MARQUES LES PLUS EXPLOITÉES PAR DES « PHISHERS » - *Quatrième trimestre 2019*

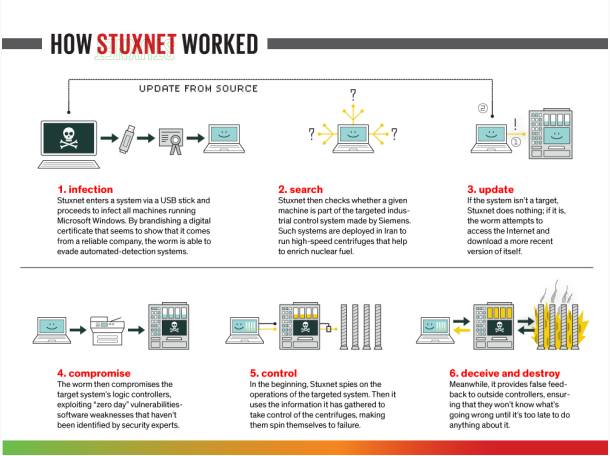
	Marque	Progression au classement sur le Q4	Nombre d'URLs Uniques	Croissance Q3 – Q4 2019
1	Paypal	=	11392	-31,2%
2	Facebook	+2	9795	-18,7%
3	Microsoft	-1	8565	-38,2%
4	Netflix	-1	6758	-50,2%
5	WhatsApp	+63	5020	+13467,6%
6	Bank of America	-1	4375	-21,5%
7	CIBC	+1	2414	-11,2%
8	Desjardins	+4	2243	-54,4%
9	Apple	-3	2126	-57,9%
10	Amazon	-1	2110	+0,6%
11	Chase	-4	2012	-14,6%
12	BNP Paribas	+3	1512	+23,1%
13	Instagram	+16	1401	+187,1%
14	Square	+19	1315	+246,1%
15	Dropbox	+1	1233	+0,7%

Fraud : CEO fraud

VIDEO

Sabotage

Stuxnet, 2010



Saudi Aramco 35 000 PC deleted in 2012.

Ransomwares: Wannacry et al. 12 may 2017

Spying

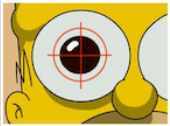
- Little Brother (person)
- Medium Brother (compagny)
- Big Brother (gouvernement)

Edward Joseph Snowden, 6th june 2013

Authentication

L'authentification

Plusieurs moyens

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Sécurité de mes mots de passe

The most commonly used authentication method

Top 25 en 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123

How has the use of passwords evolved?

Top 20 en 2024

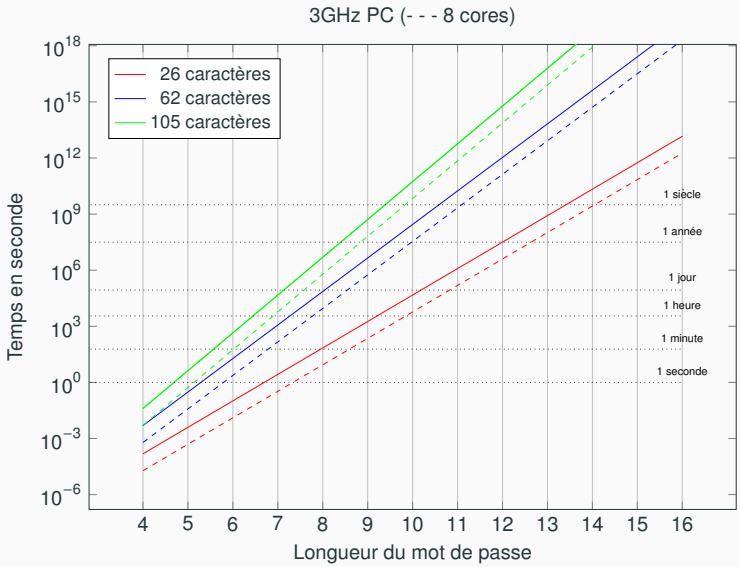
1. 123456
2. 1234567589
3. 12345678
4. password
5. qwerty123
6. qwerty1
7. 111111
8. 12345
9. secret
10. 123123
11. 1234567890
12. 1234567
13. 000000
14. qwerty
15. abc123
16. password1
17. iloveyou
18. 11111111
19. dragon
20. monkey

Passwords Brute Force

- N : nombre de caractères
- k : nombre de coeurs
- L : longueur du mot de passe
- V : vitesse du processeur en GHz
- T : temps pour énumérer tous les mots de passe en secondes

$$T = \frac{N^L}{k \times V \times 10^9}$$

Passwords Brute Force



Recommandation de l'ANSSI

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

En réalité


©Crown Copyright, 2012
www.dukeandduchessofcambridge.org


MilFlip Logon
Details
RMS
ATTENTION ALL
OMMS STUDENTS

root-me.org/fr/breve/Vol-de-donnees-password-reuse

verimag-local | sancy-local | CS253 - Web Sec... | Deus Ex Machina | Conférence PANO... | PGP | math.co.ro | MACsec Impleme...

Root Me

Rechercher

- Capture The Flag
- Challenges
- Communauté
- Documentation
- Informations
- Outils

330 visiteurs en ce moment

derniers inscrits :
ximbi emrxs nonoScOoP usap23 Desmoonde P00Y JazzyWork

Chatbox

m31z0nyx

ACCUEIL

Vol de données - password reuse

samedi 30 mai 2020

Que s'est-il passé ?

Historiquement l'association Root-Me a toujours fait confiance à tous ses contributeurs et à ce titre les membres les plus actifs jouissent généralement de droits forts.
Un administrateur de la plateforme qui a beaucoup contribué à son époque puis s'est éclipsé pour poursuivre sa vie professionnelle et familiale a été victime d'une attaque par réutilisation de mot de passe : son mot de passe est apparu dans un leak quelconque et malheureusement c'était le même que sur la plateforme Root-Me. Ce compte compromis a permis un accès illégitime au backend depuis lequel nous gérons Root-Me.

Some Advice

A password

1. should not be shared
2. should not be left lying around
3. should only be used once
4. if it is broken, it must be changed
5. it should be changed regularly
6. it is never sophisticated enough
7. size matters.

Notes:

- It is difficult to memorise 12 random characters.
- Passphrase.
- `https://keepassxc.org/`

How to Store Passwords?

Goal
We want to store passwords in a way that:

- ✓ Allows user authentication;
- ✓ Does not reveal passwords even if the database is stolen.

Comment stocker les mots de passe ?

Stockage

- In cleartext
- Haché (pwd) $\Rightarrow$ Rainbowtables !
- Haché (pwd + Salt)
- Haché (pwd + Salt-user)
- bcrypt(pwd + Salt-user)
  bcrypt = hachage plus lent ou PBKDF2
- AES(bcrypt(pwd + Salt-user), SecretKey)

Option 1: Plaintext Storage

Method

$$\mathrm{DB}[u] = \texttt{pwd}$$

where `pwd` is the password chosen by user u.

Problem

- If the database is leaked, every password is revealed immediately.
- System administrators can read user passwords.

Conclusion: Never store passwords in plaintext.

Option 2: Hashing the Password

Method

$$\mathrm{DB}[u] = h(\texttt{pwd})$$

Authentication: user sends `pwd`, system checks

$$h(\texttt{pwd}) \stackrel{?}{=} \mathrm{DB}[u]$$

Problem

- Fast hashes (h = MD5, SHA-1, SHA-256) can be reversed via **rainbow tables**:

  Precompute $h(x)$ for many x.

- Same password $\Rightarrow$ same hash $\Rightarrow$ easy to spot reused passwords.

Conclusion: Better than plaintext, but still insecure.

Option 3: Add a Random Salt

Method

$$\mathrm{DB}[u] = \left(s_u, h(s_u || \texttt{pwd})\right)$$

where $s_u \xleftarrow{\$} \{0,1\}^n$ is a random salt per user.

- Salt is stored in cleartext next to the hash.
- Prevents precomputed rainbow table attacks:

Attacker must compute $h(s_u || x)$ for each user separately.

Limitation: If h is a fast hash (e.g. SHA-256), brute force is still feasible with modern GPUs.

Option 4: Slow Hashing Functions

Method
Use a **password-based key derivation function (PBKDF)** with many iterations:

$$\mathrm{DB}[u] = \left(s_u, \mathrm{PBKDF2}_N(s_u, \mathtt{pwd})\right)$$

where N = number of iterations (e.g. 10^5).

- Makes each guess N times more expensive for the attacker.
- Recommended algorithms: **bcrypt**, **scrypt**, **Argon2**.

bcrypt

$$\mathrm{DB}[u] = \left(s_u, \mathrm{bcrypt}(s_u, \mathtt{pwd}, c)\right)$$

where c = cost parameter (2^c iterations).

Best Practice and Timing

Slow key-derivation function:

- **bcrypt(pwd, salt, cost)**: cost $\propto 2^{\text{cost}}$
- **PBKDF2(pwd, salt, iter)**: cost $\propto$ iter
- **Argon2id(pwd, salt, t, m)**: cost $\propto t \cdot m$

Goal: $\approx 200-500$ ms per hash (acceptable latency)

Method	Typical Parameters	Avg. Time[2]
SHA-256	–	$\sim 10^8$ hashes/s (too fast!)
bcrypt	cost = 12	$\sim 0.3-0.4$ s/hash
Argon2id	$t = 2$, $m = 64$ MiB	$\sim 0.2-0.4$ s/hash

Impact: attacker's offline brute-force drops from 10^8 tests/s (SHA-256) to $\mathcal{O}(10^1)$ tests/s $\Rightarrow$ **massively more expensive attack**.

[2] Sources: OWASP Password Storage Cheat Sheet, Stytch 2024, Auth0 2023

Option 5: Encrypting the Hash

Method

$$\mathrm{DB}[u] = \mathrm{AES}_K\big(\mathrm{bcrypt}(s_u, \mathtt{pwd})\big)$$

where K is a server-side secret key.

Security Considerations

- Adds a second line of defence: attacker needs both DB and K.
- If K is compromised, it can be changed (security = OPTION 4).
- Add the key management complexity.

Conclusion: Useful for very sensitive systems, but not a substitute for slow hashing.

Best Practice Summary

Recommended Approach

$$\boxed{\mathrm{DB}[u] = \left(s_u, \mathrm{Argon2}(s_u, \mathtt{pwd}, t, m, p)\right)}$$

- t = time cost (iterations)
- m = memory cost (resists GPUs/ASICs)
- p = parallelism factor

- Use **unique random salts** (s_u) per user.
- Choose parameters (t, m, p) to make hashing slow but acceptable for login (e.g. 50–200 ms).
- Regularly review parameters as hardware improves.

Short story of security

Terminology

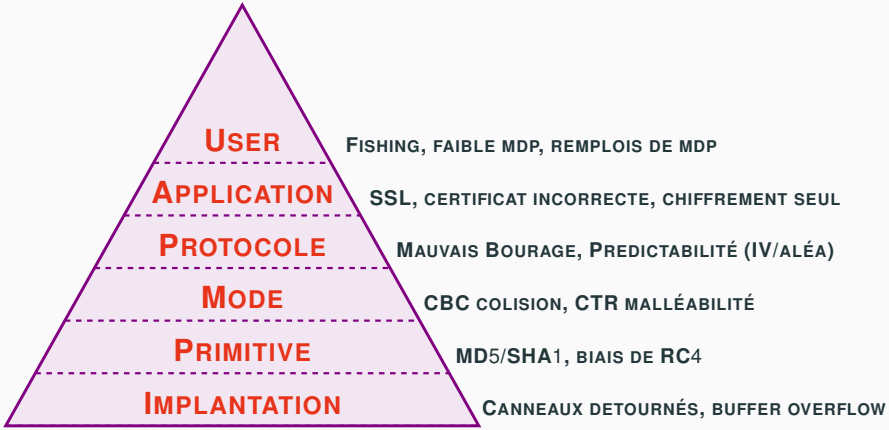
Cryptology (”Science of Secrets”) = Cryptography + Cryptanalysis

- *Cryptography*: The science that uses mathematics to encrypt and decrypt data;
- *Cryptanalysis*: The science of analysing encrypted data to recover the ”cleartext” version;
- $\neq$ *Steganography*: The method of hiding the very existence of a message;
- *Cryptographic system (or cryptosystem)*: Cryptographic algorithm + key management + protocols.

Reference: Request for Comments RFC 2828. ”Internet Security Glossary”. May 2000. `https://www.ietf.org/rfc/rfc2828.html`

Cryptography and Security

- Cryptography is one element in building secure systems
- There are security issues at every level:



Transposition Cipher

Permutation

YPCOITARPHRGE

Scytale

Caesar Cipher (a shift cipher)

cryptanalyse
↓ +3
fubswdqdobvh

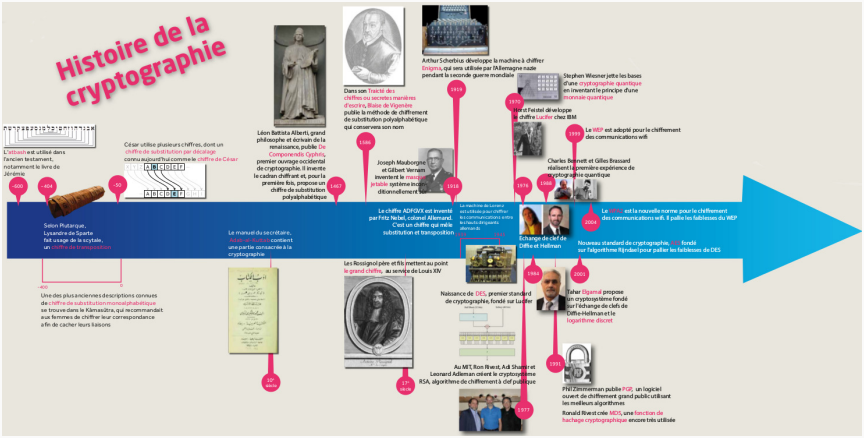
Vigenère Cipher (block cipher)

We take a key (here ”bonjour”) and ”add” the letters. If the key is too short, it is repeated until reaching the right length.

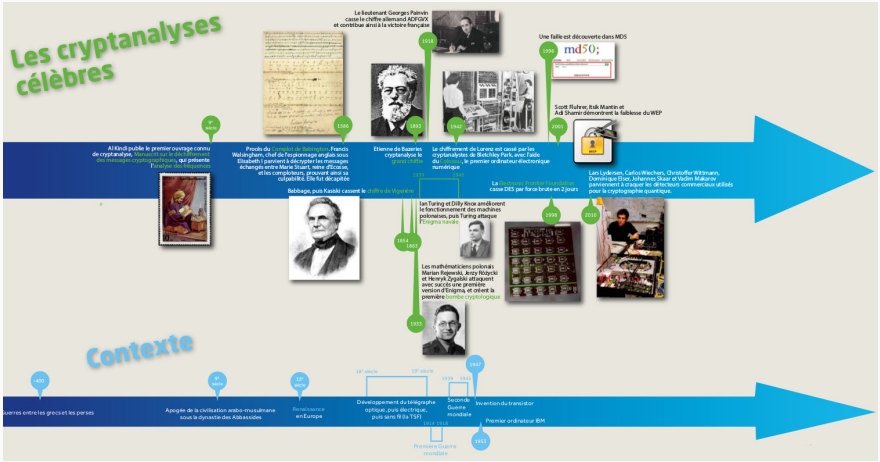
	L	A	F	L	E	U	R	R	O	U	G	E
+	B	O	N	J	O	U	R	B	O	N	J	O
	K	M	S	C	Q	A	A	Q	A	H	X	Q

Enigma (stream cipher)

History of Cryptography



History of Cryptanalysis



Le téléphones rouge

The One-Time Pad

Inputs/Outputs:

- Message $m \in \{0,1\}^\ell$ (plaintext), message space: $\mathcal{M} = \{0,1\}^\ell$
- Key $k \in \{0,1\}^\ell$, key space: $\mathcal{K} = \{0,1\}^\ell$
- Ciphertext $c \in \{0,1\}^\ell$, ciphertext space: $\mathcal{C} = \{0,1\}^\ell$

Algorithms:

- Encryption: $Enc_k(m) = m \oplus k$
- Decryption: $Dec_k(c) = c \oplus k$
- Correctness: $Dec_k(Enc_k(m)) = (m \oplus k) \oplus k = m$

Advantages:

- Used during the Cold War
- Suitable for short messages/secrets
- Perfectly secure (information-theoretic security)

Drawbacks:

- Key must be as long as the message
- Can only be used once
- Key must be uniformly random

“Crypto Wars” in France

Conflict between national security and privacy (1980 – today)

- **1985**: The DST and DGSE pushed to ban the civilian use of cryptography.
- **1986**: Decree n°86-250 of 18 February: cryptography was classified as a weapon of war  , strictly regulated.
- **1996**: Law n°96-659 (26 July): opening up, but under declaration and prior authorisation.
- **2004**: Law for Confidence in the Digital Economy: *democratisation* of encryption, but mandatory declaration to the State.
- **2016-2017**: Debate on “backdoors” after the 2015 terrorist attacks. The President supported better access to encrypted communications, opposed by ANSSI, CNIL and CNNum.
- **2019**: Court ruling reaffirming the right to strong encryption.

What Future for Cryptography?

- **Crypto Wars 2.0?** *Towards a renewed debate on backdoors and government access to encrypted data.* Global context: Clipper Chip (USA), export controls, recent debates on end-to-end encryption (WhatsApp, Messenger, iMessage).
- **Post-Quantum Cryptography** Preparing for the future in the face of quantum computers

Cryptography and Society: A Close Link

- **Energy and Resource Consumption**: ecological impact of infrastructures and blockchains.
- **Privacy**: age verification, digital identity, fighting mass surveillance.
- **Ethics and Regulation**: balance between public security and fundamental freedoms.

`https://www.activism.net/cypherpunk/manifesto.html`