La cryptologie
● Définitions

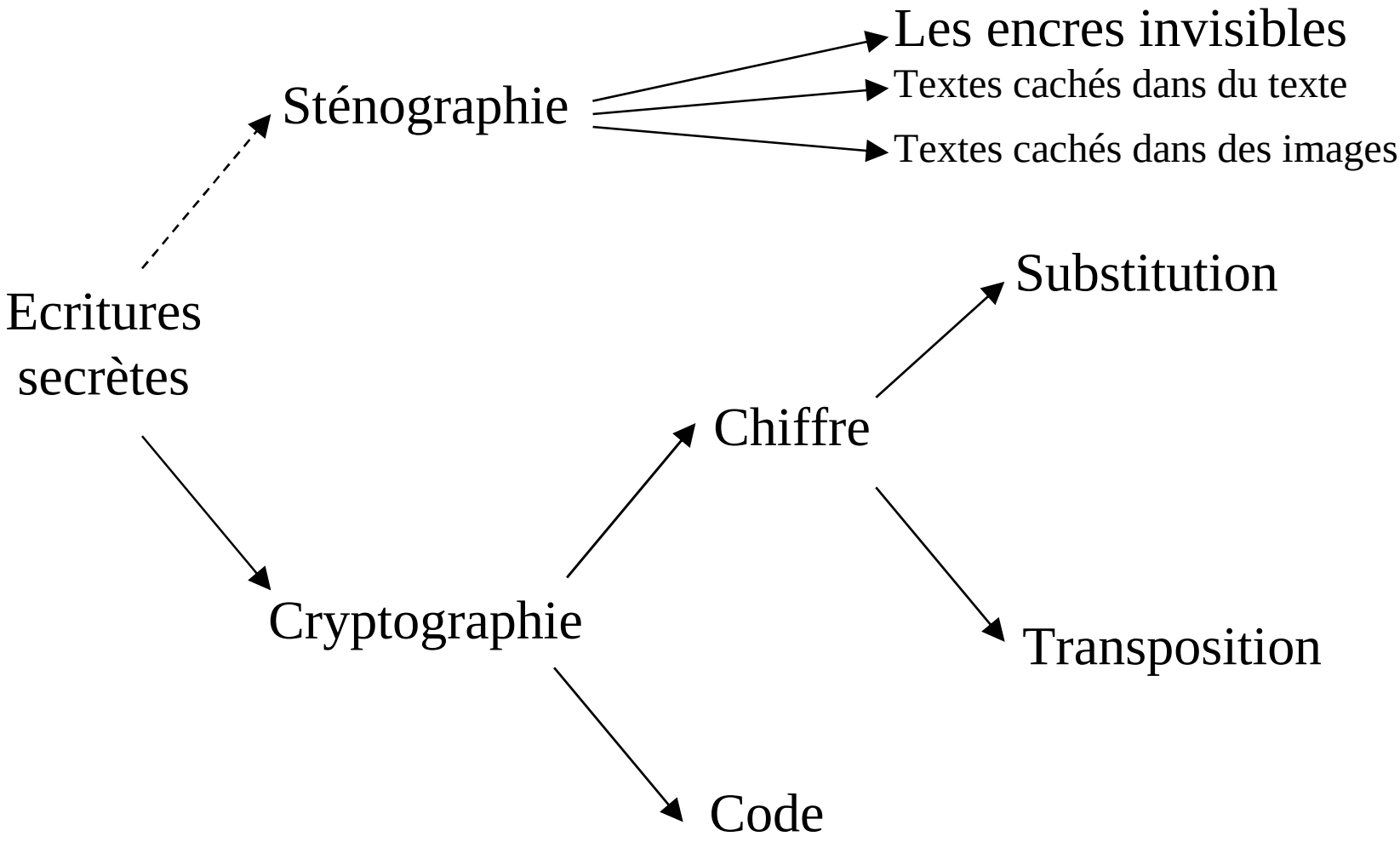
La cryptologie

- **La cryptologie**
  - La cryptologie, étymologiquement la science du secret. Cette science englobe la cryptographie — l'écriture secrète – et la cryptanalyse – l'analyse de cette dernière.
- **La cryptographie**
  - La cryptographie est la science des « écritures secrètes ».
  - On va modifier un texte écrit en vue de le rendre incompréhensible à ceux qui n'ont pas à le connaître.
- **La cryptanalyse**
  - La cryptanalyse est la science des « briseurs de code ». L'objectif est de comprendre la signification des messages transmis sans connaître à priori les règles qui l'ont rendu incompréhensibles.

Cryptographie – Un peu de vocabulaire

- **Définition**
  - Chiffrer — Transformer un message clair en un message dit chiffré, incompréhensible par tout un chacun en utilisant des règles connues que du ou des correspondants.
  - Déchiffrer — Réaliser l'opération inverse.
  - Cryptogramme — Le message chiffré.
  - Décrypter — Trouver le clair du message sans connaître a priori les règles utilisées par les correspondants légitimes.
  - Cryptographe ou chiffreur — Personne qui chiffre ou déchiffre.
  - Cryptanalyste — Personne pratiquant la cryptanalyse.

La cryptographie



La cryptographie – Les méthodes de transposition

- **Définition**
  - On découpe le message que l'on veut transmettre en petites unités et on mélange les unités selon des règles établies et connues des seuls correspondants. Les unités sont le plus souvent des lettres mais peuvent aussi être des mots complets.
- **Exemple de méthode**
  - Message clair: L'humour, la politesse du désespoir. (Oscar Wilde)
  - `L U O R A O I E S D D S S O R`
`H M U L P L T S E U E E P I`
  - Message chiffré (par groupe de 5 lettres):
`LUORA OIESD DSSOR LUORA OIESD DSSOR`

Cryptographie – Chiffre par substitution

- **Définition**
  - On découpe le message que l'on veut transmettre en petites unités de taille fixe, par exemple par lettre et on substitue chaque unités par une autre selon des règles connues des correspondants.
- **Exemple de méthode**
  - Alphabet en clair et alphabet de substitution (à l'envers)
    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    ZYXWVUTSRQPONMLKJIHGFEDCBA
  - Message en clair: Ne cédez pas à la colère vengez-vous. (Gandhi)
  - Message chiffré:
    MV XVWVA KZH Z OZ XLOVIV EVMTVA-ELFH

Cryptographie – Les codes

- **Définition**
  - En cryptographie, les codes (on dit aussi répertoires ou dictionnaires) sont des systèmes de substitution dont les unités substituées sont de taille variable. Ce peut être des lettres, des syllabes, des mots ou des phrases. Les unités de substitutions sont le plus souvent des nombres (d'où le terme « chiffrer »), mais peuvent aussi être des multi-grammes composés chacun de 2, 3, 4 ou 5 lettres.
  - Les deux formes de codes:
    - Les codes ordonnés
    - Les codes à bâtons rompus (ou désordonnés)
- **Les codes surchiffrés**
  - Pour améliorer la sécurité, on peut faire subir une méthode de chiffrement (substitution ou transposition) au résultat du codage.

La stéganographie

- **Définition**
  - La stéganographie est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit.
  - Les encres invisibles sont une technique de stéganographie.
- **Exemple**
  - Monique, une résistante normande envoie ce message (transmis ensuite à Londres) :
    1 kilo de poires, 2 livres de cerises, 1 kilo de pommes,
    5 kilo de tomates, 5 courgettes.
  - Signification: Il y a 12 nouveaux canons de 155 mm installés.

Cryptographie – Les chiffres – Les principes de Kerckhoff

- **Introduction**
  - Auguste Kerckhoffs, en fin XIX a décrit les qualités d'un bon chiffre militaire.
- **Les desiderata d'un chiffre militaire**
  - Le système doit être matériellement, sinon mathématiquement indéchiffrable.
  - Il faut qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
  - La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
  - Il faut qu'il soit applicable à la correspondance télégraphique.
  - Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
  - Il faut 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.

Cryptographie – Les chiffres – Le concept de clé

- **Introduction**
  - Auguste Kerckhoffs, dans sa description d'un bon chiffre militaire invente presque la notion de clé.
- **Définition d'une clé de chiffrement**
  - Soit un algorithme de chiffrement, par exemple le Vigenère. La sécurité de l'utilisation de ce système ne doit pas reposer sur l'ignorance par l'ennemi de l'usage de ce système. En clair, un système de chiffrement n'a pas besoin d'être secret pour apporter la sécurité des transmissions.
  - Le seul élément qui doit être secret (mais partagé par les correspondants), doit être la « clé ». C'est un élément variable du processus de chiffrement.

Histoire de la cryptologie

Histoire de la cryptologie – Les grandes périodes

- **Le début (antiquité à la première guerre mondiale)**
  - Apparition des nomenclatures ancêtres des codes.
  - Substitutions et transpositions simples.
- **La cryptologie mécanique, électronique (1ere et 2eme GM)**
  - Les machines à chiffrer se répandent.
  - Les systèmes électroniques, les ordinateurs reproduisent les algorithmes des méthodes manuelles ou des machines.
- **La cryptologie moderne (à partir des années 1970)**
  - Utilisation des registres à décalage (cryptographie par blocs).
  - La cryptographie à clé publique.

Histoire de la cryptologie – L'antiquité

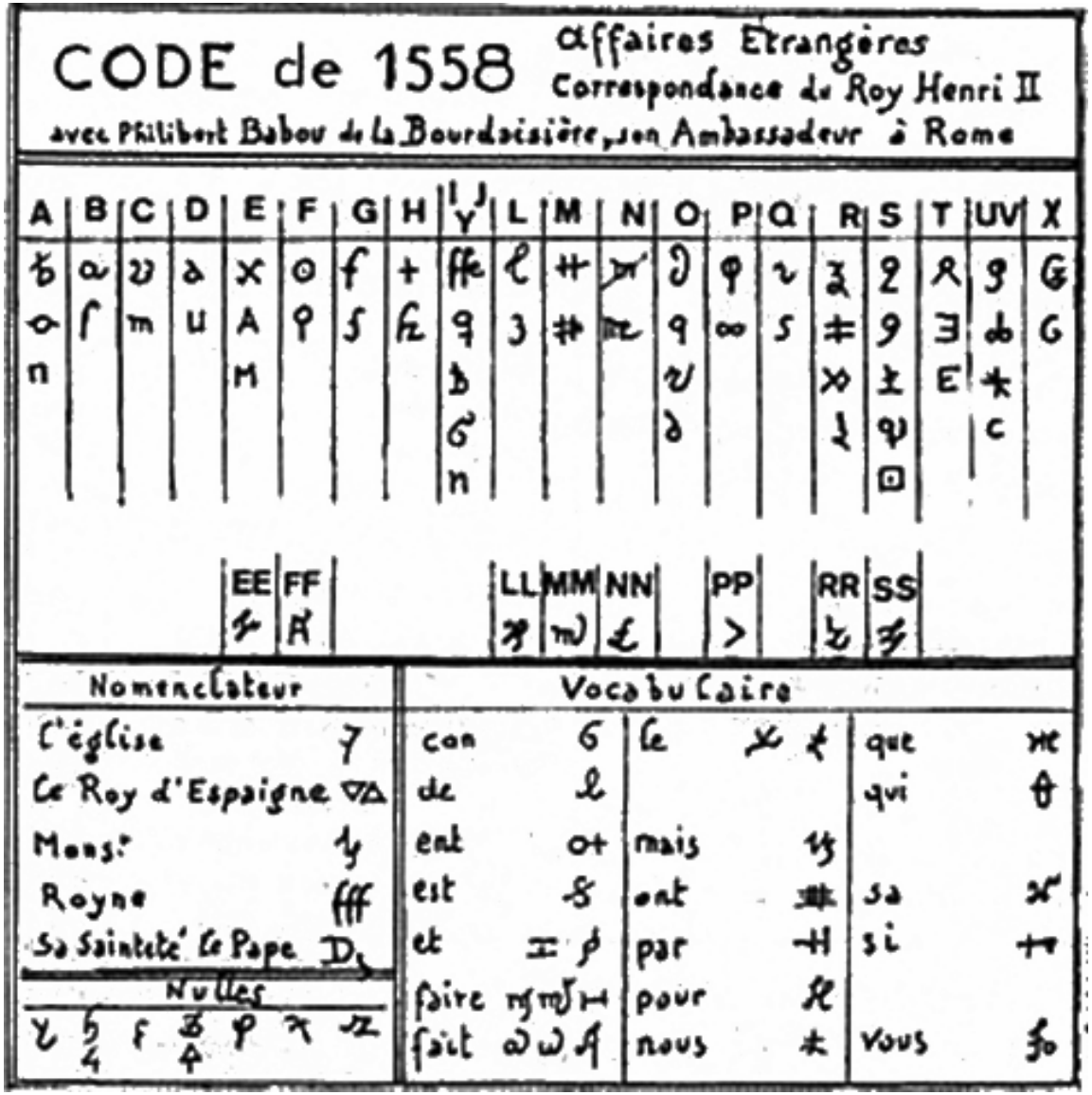
- **La scytale (méthode de transposition)**
  - C'est un bâton dont le diamètre sert de clé : les correspondants doivent avoir un bâton de diamètre identique.
  - On enroule une bande de tissu autour et on écrit le message dans le sens de la longueur sous forme de plusieurs lignes.

- **La méthodes de Jules césar (méthode de substitution)**
  - On décale chaque lettre de trois positions.

Histoire de la cryptologie – La renaissance

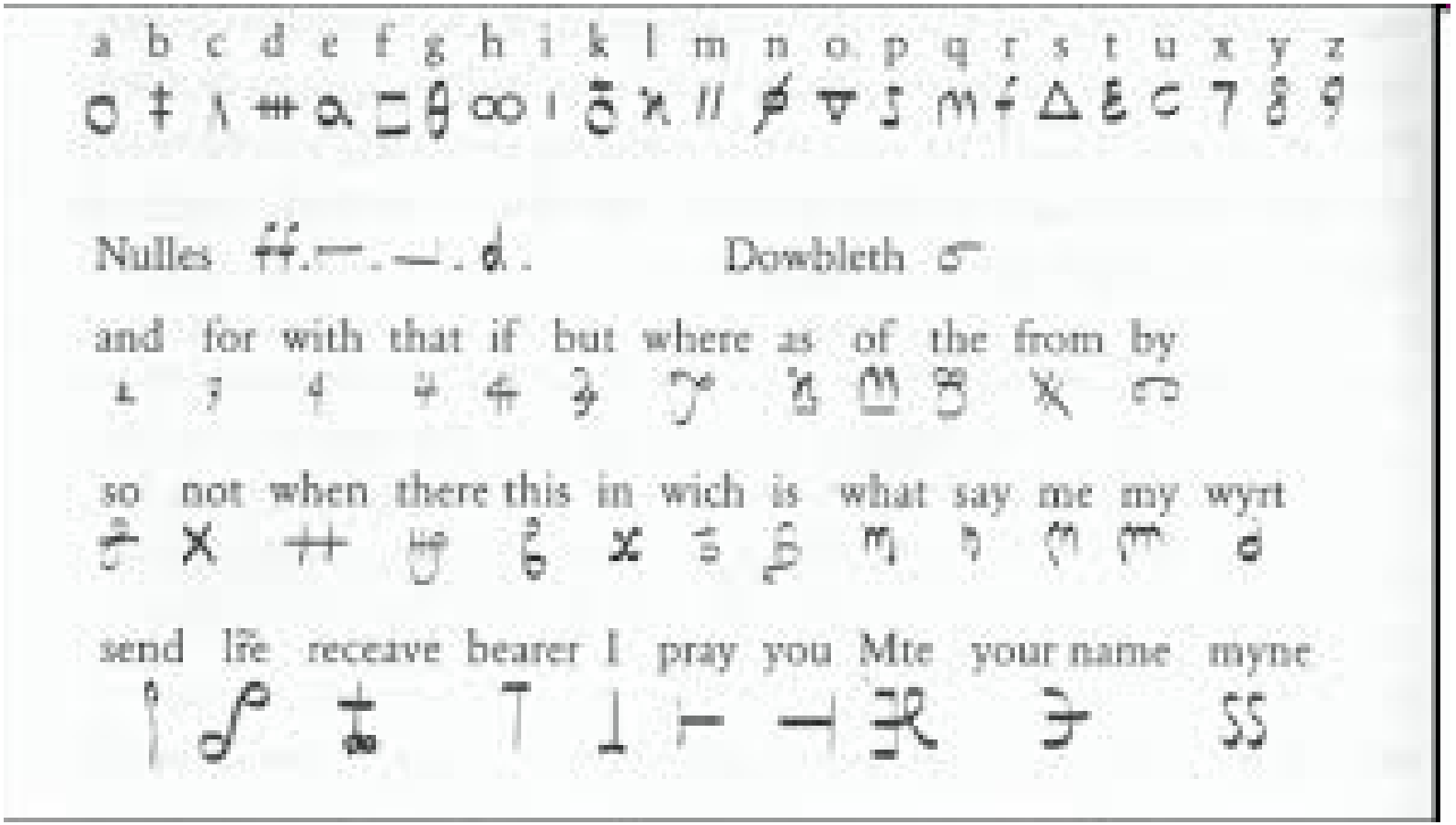
- **Le contexte**
  - Les ambassadeurs doivent communiquer avec leur métropole. Le pape doit communiquer avec ses nonces.
  - Les cabinets noirs des différents pays essayent de casser les codes des autres ambassadeurs ou des nonces.
- **Les méthodes cryptographiques utilisées**
  - La première méthode utilisée a été de simple alphabets de substitutions. Rapidement ils deviennent des « nomenclateurs » qui ajoutent à l'alphabet de substitution les mots fréquemment utilisés. Ce sont les ancêtres des codes.
  - Les chiffres aussi apparaissent et se complexifient (disque d'Alberti, système de Porta, Vigenère, …).

Histoire de la cryptologie – Nomenclateur



Histoire de la cryptologie – Nomenclateur

Nomenclateur de Mary, reine d'Ecosse. Les lettres chiffrés utilisant ce système ont été interceptées et décodées. Elles serviront de preuve dans son procès pour complot contre la reine Elisabeth d'Angleterre. La reine Mary finira décapitée en 1587.

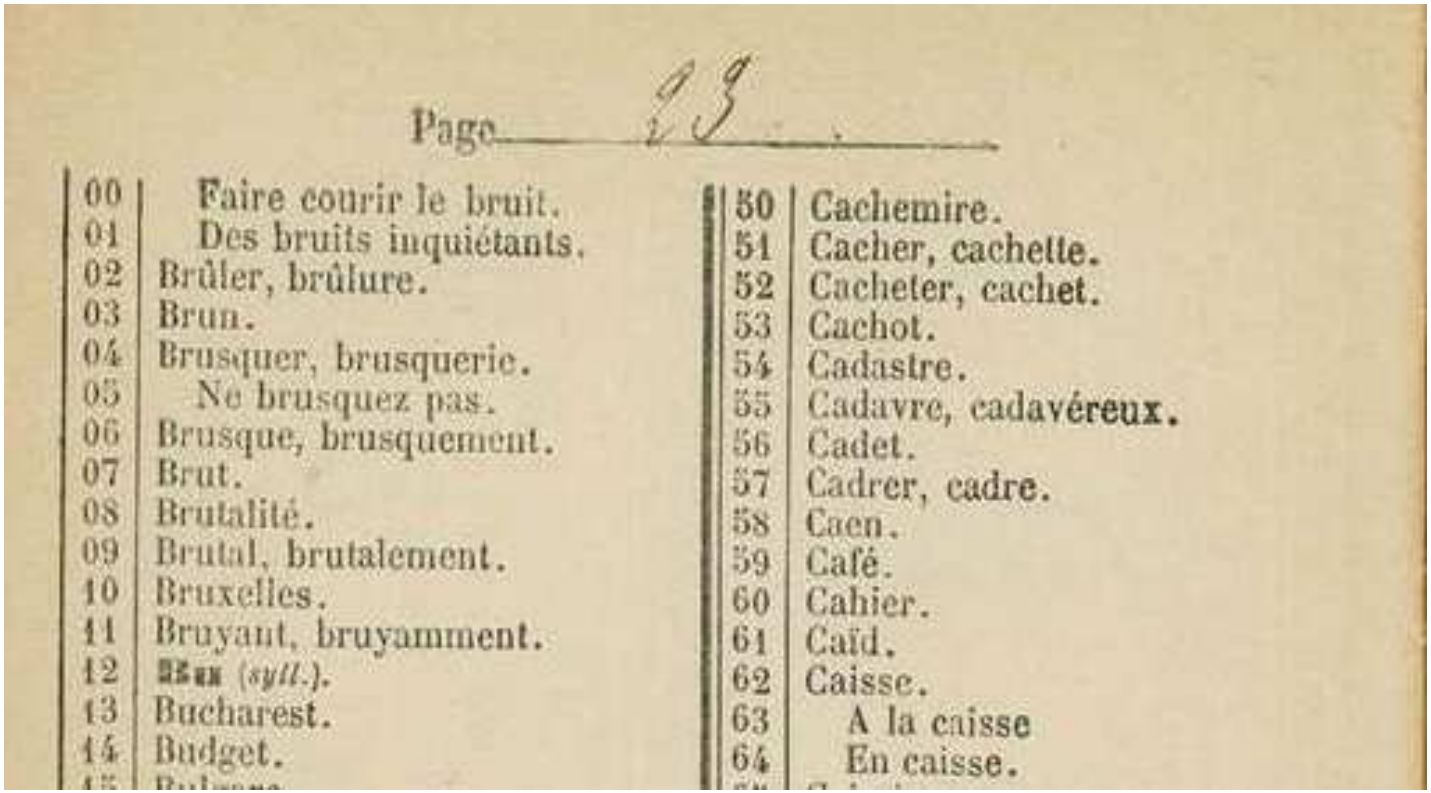


Histoire de la cryptologie – XVII à début XX: les codes

- Les nomenclateurs deviennent de plus en plus complexe et en final finissent par devenir des codes.

Histoire de la cryptologie – XVII à début XX: les codes

- Avec l'apparition du télégraphe, les sociétés utilisent les codes pour la confidentialité des échanges mais aussi pour réduire les coûts (on paye au mot) : un texte codé est plus court qu'un texte clair. Exemple le « Sittler » (fin XIX) : -- « café » est codé 2359.



Page 23

00	Faire courir le bruit.
01	Des bruits inquiétants.
02	Brûler, brûlure.
03	Brun.
04	Brusquer, brusquerie.
05	Ne brusquez pas.
06	Brusque, brusquement.
07	Brut.
08	Brutalité.
09	Brutal, brutalement.
10	Bruxelles.
11	Bruyant, bruyamment.
12	[illegible] (*syll.*).
13	Bucharest.
14	Budget.
50	Cachemire.
51	Cacher, cachette.
52	Cacheter, cachet.
53	Cachot.
54	Cadastre.
55	Cadavre, cadavéreux.
56	Cadet.
57	Cadrer, cadre.
58	Caen.
59	Café.
60	Cahier.
61	Caïd.
62	Caisse.
63	A la caisse
64	En caisse.

Histoire de la cryptologie – Les codes surchiffrés (XIX et XX)

- Pour améliorer la sécurité, les codes sont surchiffrés avec des méthodes « additives » ou en utilisant des transpositions.

Code text	50864	04330	13024	62895	65165	73032
Additive	43415	27267	02983	26631	22763	35178
Resulting Cipher text	93279	21597	15907	88426	87828	08100
Code	33317	27303	43314	00093	07002	04485
Additive	34418	11312	91904	11751	45729	92241
Cipher	67725	38615	34218	11744	42721	96626
Code	25266	00147	62570	88382	50451	15374
Additive	96193	96401	39302	02492	03638	62865
Cipher	11359	96548	91872	80774	53089	77139
Code	50045	19355	54454	15475	75481	00001
Additive	41197	09021	58046	03071	95826	70990
Cipher	91132	18376	02490	18446	60207	70991
Code	12337	32831	21396	11070	00007	21402
Additive	24126	99760	39549	00462	93615	87426
Cipher	36453	21591	50835	11432	93612	08828

Histoire de la cryptologie – OTP : Le système incassable

- **Introduction**
  - L'OTP (One-Time-Pad), en français clé à usage unique est un système cryptographique apportant une sécurité absolue.
  - Le principe est simple, on utilise une méthode (par exemple le Vigenère) auquel on applique une clé aléatoire et jetable de la taille du message (on utilise une nouvelle clé pour chaque message). Il fut inventé lors de la 1ere GM.
  - Le « Téléphone Rouge » utilise cette technique.
- **Inconvénient**
  - Les correspondants doivent produire, via des processus physiques aléatoires [exemple un compteur de radiations] et échanger (au préalable) autant de clés que d'information à transmettre.

Histoire de la cryptologie – La machine Kryha (1920)

Histoire de la cryptologie – La machine Enigma (2ème GM)

Histoire de la cryptologie – La machine M-209 (2ème GM)

Histoire de la cryptologie – La machine Fialka (1956-1990)

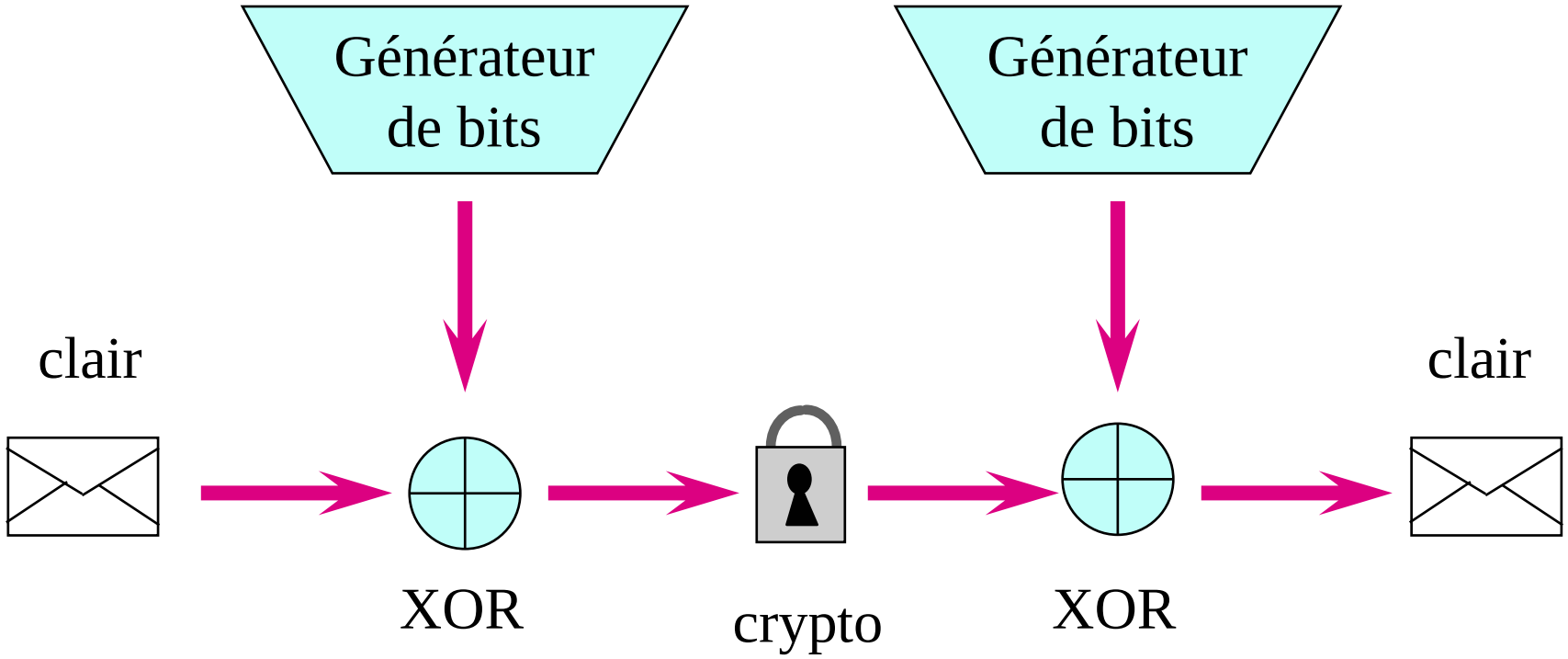
Histoire de la cryptologie – La cryptographie moderne

- **Introduction**
  - Dans les années 1970, la cryptographie sort du monde secret militaire et diplomatique. L'usage des ordinateurs et des réseaux nécessite de nouvelles méthodes incassables et ouvertes adaptées à ces environnements.
  - Les algorithmes par blocs basés sur les registres à décalage se répandent ainsi que la cryptographie à clé publique.
- **Lucifer**
  - Lucifer est une famille d'algorithmes de chiffrement par bloc développés par Horst Feistel et ses collègues d'IBM. Il s'agit d'une des premières méthodes de chiffrement moderne destinée à un usage civil. Lucifer fut le précurseur direct de DES. Une des versions, DTD-1, fut utilisée pour une banque en ligne (e-banking) durant les années 1970.

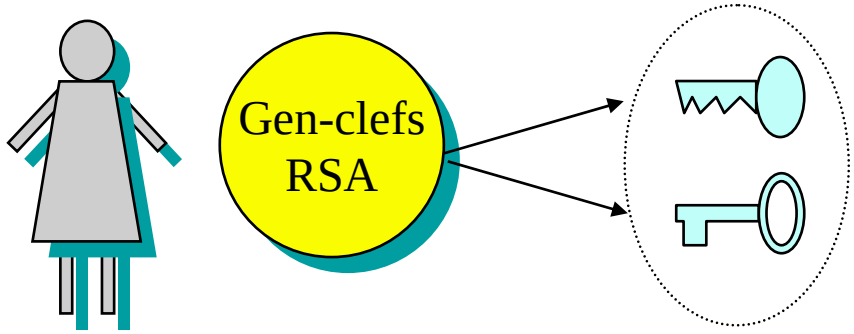
Qualités d'un algorithme (de type symétrique)

- **Qualités**
  - Il doit résister à une attaque mathématique.
  - Il doit résister à une attaque exhaustive (taille des clés > 110 bits)
  - Il doit aussi être simple (pour déceler des failles) et rapide.
- **Les principaux algorithmes et leur taille de clé**
  - AES (le standard actuel) 128, 192 ou 256 bits
  - 3DES 112 bits
  - DES (l'ancien standard) 56 bits (« cassée » en 1999)
  - RC4 40 à 256 bits

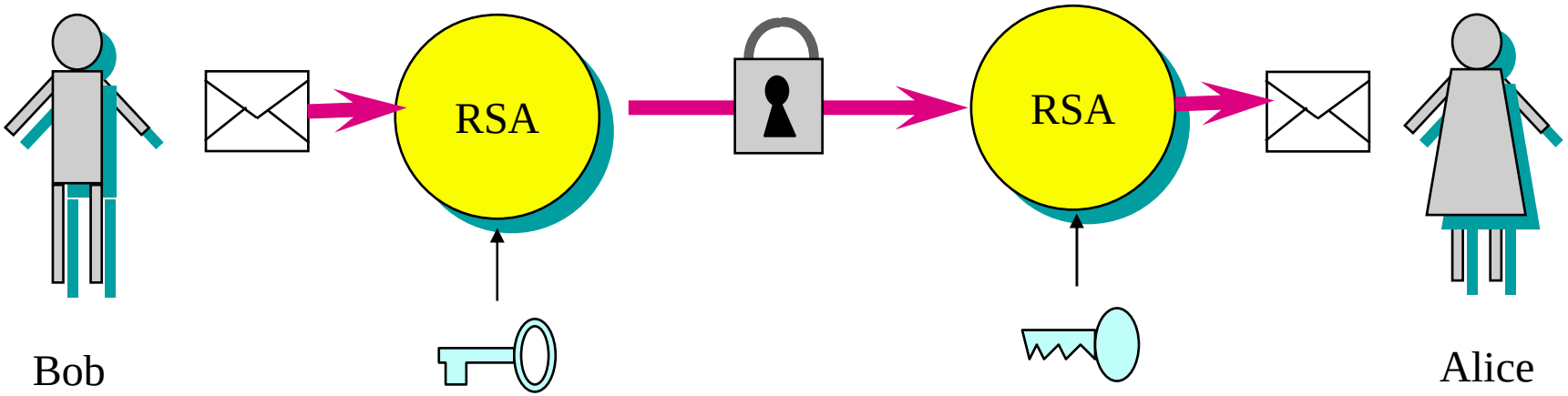
Chiffrement par flux (stream cipher)



Les algorithmes de chiffrement à clé publique



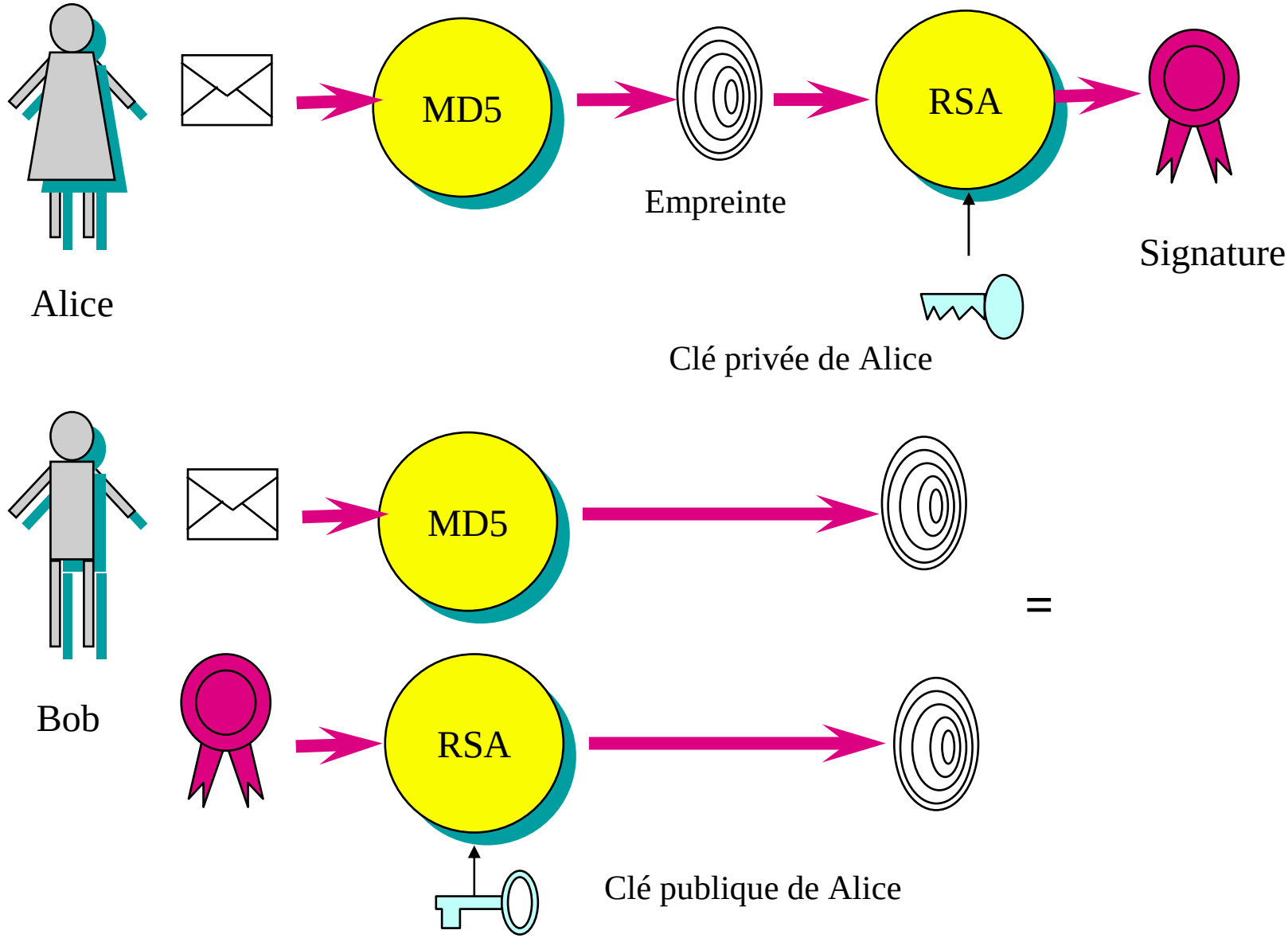
Alice génère un couple
(clé publique, clé privée)



Clé publique de Alice

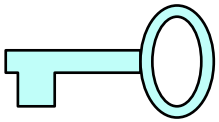
Clé privée de Alice

La signature numérique

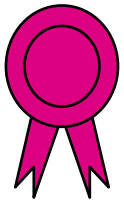


Les certificats X509

Version : 3
Numéro de série : 0128A2
Algorithme signature : MD5-RSA
Emetteur : thawte.com
Validité : 4/7/00 au 18/7/01
Objet : secure.bletchleypark.org.uk
Algorithme clé : RSA



« Clé publique et signature »



Qualités d'un algorithme (de type asymétrique)

- **Qualités**
  - Il doit résister à une attaque mathématique.
  - Il doit résister à une attaque ciblée,
    par exemple, le RSA doit résister à une attaque par factorisation
    (taille des clés >= 2048 bits)
- **Les principaux algorithmes**
  - Diffie-Hellman (uniquement pour établir un secret à la volée)
  - RSA
  - DSA
  - ECDSA (variante de DSA utilisant les méthodes elliptiques)

Les protocoles cryptographiques

- **La théorie**

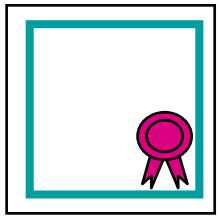
  En cryptologie, le plus important ce sont les protocoles cryptographiques car ils résolvent des problèmes concrets de sécurité, par exemple :

  - Echange de données en réseau de manière sécurisée
  - Acheter sur Internet
  - Jouer au Poker en réseau
  - Voter de manière électronique

  Ils sont construits à partir de différents algorithmes cryptographiques, par exemple SSL utilise AES, SHA, RSA, …

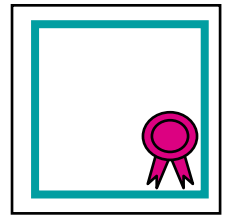
- **Exemples de protocoles**
  - Echange de données chiffrées et authentifiée: SSL/TLS
  - Courriers électroniques: PGP,S/MIME

SSL – Le protocole

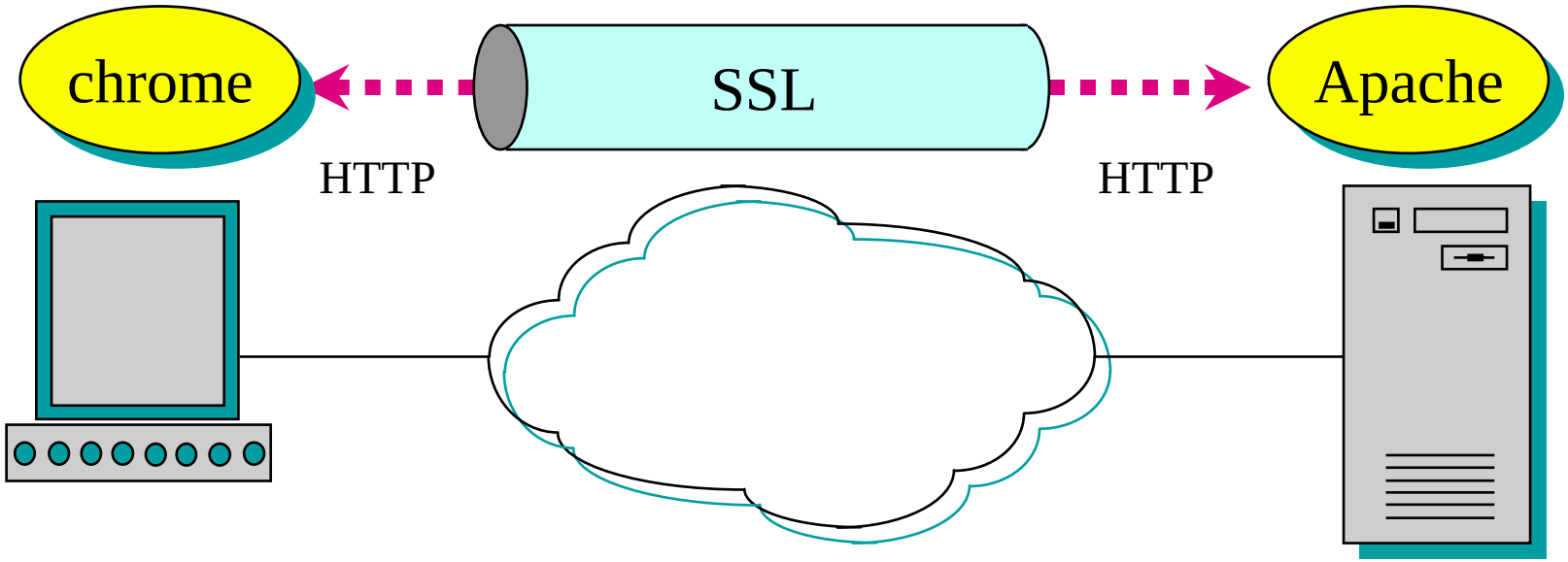


Certificat d'une autorité (CA)

Le navigateur crée une clé AES qu'il transmet au serveur via RSA. Ensuite les échanges ont lieu en AES.



Certificat du serveur



URL: https://serveur

serveur

La transmission quantique

- **Description**
  - La cryptographie quantique cherche à simplifier les échanges de données chiffrées de manière symétrique.
  - Le gros problème quand on utilise une méthode symétrique est la transmission de la clé secrète. L'usage des systèmes à clé publiques est en final complexe.
  - En utilisant les lois de la physique quantique, une information (par exemple une clé secrète) peut être transmise sur un canal publique tout en étant capable de détecter un espionnage éventuel. S'il n'y a pas eu espionnage, l'information (par exemple une clé secrète) peut être extraite de la transmission, et utilisée dans tout algorithme de chiffrement symétrique afin de transmettre un message.

Blockchain, Bitcoin et cryptomonnaie

- **Blockchain**
  - Une (ou un) blockchain, est une technologie de stockage et de transmission d'informations sans organe de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne. L'ensemble est sécurisé par cryptographie.
- **Cryptomonnaie (basée sur les Blockchain)**
  - Une cryptomonnaie est une monnaie émise de pair à pair, sans nécessité de banque centrale, utilisable au moyen d'un réseau informatique décentralisé.
  - Bitcoin: C'est la cryptomonnaie la plus connue. Il est basé sur un code informatique en Open Source publié en 2009.

La cryptologie

- La cryptanalyse

Attaque de la méthode de JC : Attaque exhaustive

- **Principe de l'attaque exhaustive**
  - Si on connaît la méthode de chiffrement, on peut en déduire toutes les clés possibles.
  - L'attaque exhaustive consiste à tester toutes ces clés.
- **La taille d'une clé**
  - En supposant qu'il y a 26x26x26 clés. On exprime la taille d'une clé (en fait le nombre de clés) en puissance de 2: 2 ** 15 > 26**3, donc la taille de la clé est 15.
  - Actuellement une méthode de cryptographie dont la taille est inférieure à 80 est considérée comme peu sure.
  - La taille de la clé de la méthode de JC est de 5 (en fait il y a 25 décalages possibles). Les clés AES les plus petites sont de 128.

Attaque de la substitution simple : Analyse de fréquences

- **Analyse de fréquences des lettres**
  - En français, toutes les lettres n'ont pas la même probabilité:

E	17 %	N	7.5 %
S	8.5 %	T	7 %
A	8. %	I	7 %

    (les lettres les plus fréquentes forment le mot ESANTIRULO)
- **Les bigrammes les plus fréquents**
  - ES DE LE EN RE NT ON ER
    TE EL AN SE ET LA AI IT
    ME OU EM IE
- **Quelques trigrammes fréquents**
  - ENT LES EDE DES QUE AIT LLE SDE
    ION EME ELA RES MEN ESE DEL ANT
    TIO PAR ESD TDE

La méthode du mot probable (Crib)

- **Description**
  - La méthode du mot probable (ou en anglais « Crib ») consiste à supposer la présence d'une chaîne de caractères (qui peut être un simple mot) comme étant la signification d'une partie particulière du cryptogramme, par exemple son début.
- **Exemples**
  - Bazières a cassé le code de Louix XIV en supposant que la suite de codes la plus fréquente correspondait au mot « ennemi ».
  - Durant la seconde guerre mondiale beaucoup de clés Enigma on été cassées car un des messages les plus fréquents était: «nichts zu berichten » (rien à signaler). Dés que l'on connaît la clé, tous les messages de la journée pouvaient être déchiffrés.

L’indice de coïncidence

- **Description**
  - L'indice de coïncidence est une technique de cryptanalyse inventée par W.F. Friedman en 1920.
  - L'indice permet de savoir si un texte a été chiffré avec un chiffre mono alphabétique ou un chiffre poly-alphabétique en étudiant la probabilité de répétition des lettres du message chiffré. Il donne également une indication sur la longueur de la clé.
  - Formule: $\Sigma (F[i]* (F[i]-1)) / (N * (N-1))$

    Le i varie de 0 à M (le nombre de lettres de l’alphabet).
    F[i] étant le nombre d’occurrence de la ième lettre de l’alphabet.
    N étant le nombre de lettres du message.
  - Valeurs: Français : 0.078, Anglais: 0.067, texte aléatoire: 0.0385

Références

- **La cryptologie ludique (en français)**
  - Didier Muller - Ars Cryptographica – Table des matières
    https://www.apprendre-en-ligne.net/crypto/activites/index.html
  - dCode.FR
    https://www.dcode.fr/
- **Histoire de la cryptologie**
  - Wikipédia – Histoire de la cryptologie
    Remarque: l'article possède beaucoup de liens
    https://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie
- **Cryptologie et mathématiques**
  - Cryptographie – Exo7 (maths, crypto, algorithmes, …)
    http://exo7.emath.fr/cours/ch_crypto.pdf
- **Un livre sur l'histoire de la cryptologie:**
  Siman Singh – Histoire des codes secrets