Introduction à la cryptographie (Cours 1) .

Michaël Quisquater (Maître de Conférences,UVSQ)

Première partie I

Introduction à la cryptographie d'hier

Plan de la première partie

Supports de conservation d'informations d'hier

Tablettes de cire :

Papyrus, parchemin, papier :

Moyens de communication d'hier

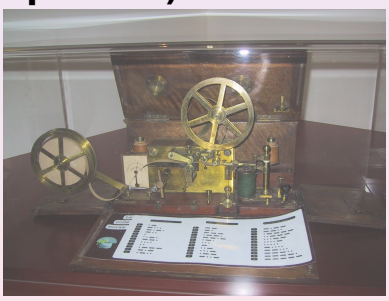
Messager militaire (ex. marathon : 490 av. J.-C.) :

Service postal (relais de chevaux : 500 av. J.-C.) :

Moyens de communication d'hier (suite)

Télégraphe optique (1690 ap. J.-C.)

Electrique : Morse (1832 ap. J.-C.)



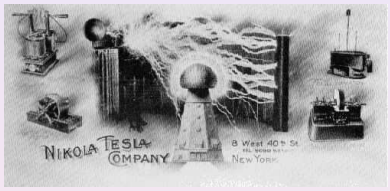
Moyens de communication d'hier (suite)

Télégraphe sans fil (Guglielmo Marconi, 1896) :

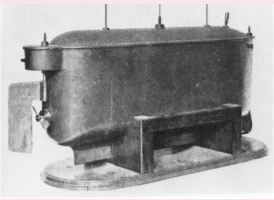
Remarque : Guglielmo Marconi s'est appuyé sur les travaux de Hertz, Popov, Branly et Lodge.

Moyens de communication d'hier (suite)

Radio (Nikola Tesla, 1892) :



Bateau (arme) téléguidé (1898) :



Besoins ?

- Sécuriser du contenu (exemple : rendre illisible un plan de construction)
- Efficacité (transmettre ou écrire le minimum)
- Rendre la communication fiable
- Rendre la communication confidentielle
- Avoir une certaine assurance de qui nous envoie un message.

Modèle : Chaîne de codage

Remarque :

- Codage entropique (1), cryptographique (2) et de canal (3)
- L'ordre de ce codage est très important (toutes les étapes ne sont pas toujours utilisées)

Codage entropique, codage cryptographique, codage de canal

Codage entropique :

Le codage entropique consite à compresser les données afin d'enlever la redondance de celles-ci.

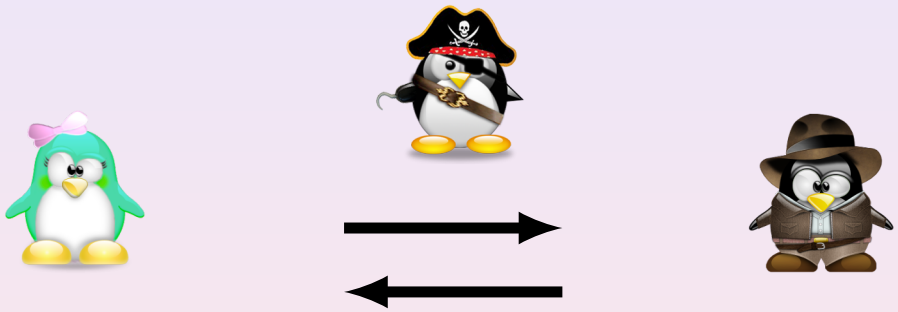
Codage cryptographique :

Le codage cryptographique consiste à traiter les données afin d'assurer certaines fonctions de sécurité.

Codage de canal :

Le codage de canal consiste à ajouter de la redondance dans les données ce qui permet de corriger ou détecter des erreurs (+remarque).

Modèle de communication à deux intervenants du point de vue du cryptographe

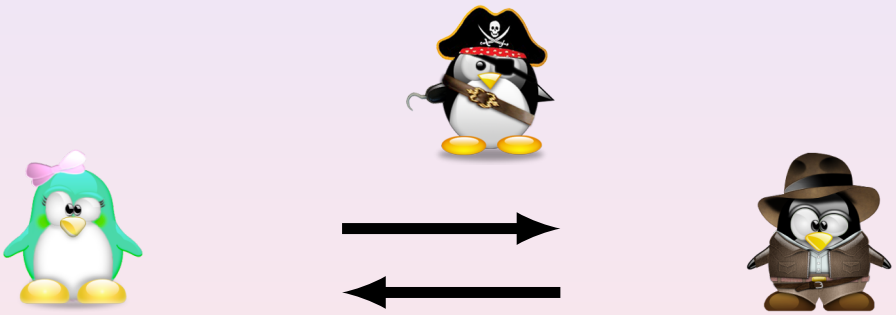


Hypothèses :

- Deux intervenants en présence d'un pirate.
- Les deux intervenants peuvent se rencontrer avant l'ensemble des échanges afin de se mettre d'accord sur un ensemble de paramètres.

Enjeux de la cryptographie d'hier : Confidentialité

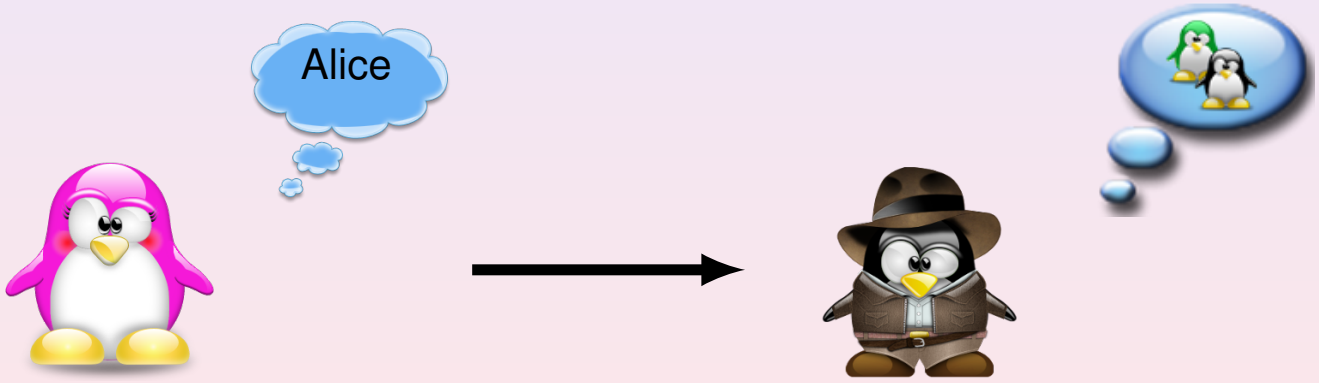
S'assurer du caractère secret de l'information



Stockage de données sécurisé

Enjeux de la cryptographie d'hier : Authentification des personnes

Des personnes : être capable de vérifier qu'une personne est bien celle qu'elle prétend être

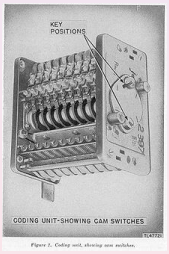


Enjeux de la cryptographie d'hier : Authentification des personnes

"Identification" friend or foe (amie eu ennemie) : IFF.

Mise en place : Seconde Guerre mondiale

Objectif : reconnaître les avions "amis" et déterminer leur cap ainsi que leur distance.



Enjeux de la cryptographie d'hier (suite)

Principe : Pour démarrer la procédure d'identification l'opérateur au sol commute la fréquence d'impulsions de son radar de 3 750 Hz à 5 000 Hz. Le récepteur radio embarqué de l'avion décode ce changement et lance l'émission de son propre code. Avant le décollage, deux clefs mécaniques de 10 bits chacune sont insérées dans le lecteur visible sur la photographie

Terminologie

Etymologie du mot cryptographie : Vient du grec, kruptos qui signifie "secret " et graphein qui signifie "écriture" .

Vocabulaire

Cryptographie : Conception de primitives permettant d'assurer l'un (ou plusieurs) des 4 enjeux.

Cryptanalyse : Art de mettre en défaut des primitives cryptographiques

Cryptologie : Science qui étudie la cryptographie et la cryptanalyse

Terminologie (suite)

- Message clair / Message chiffré
- Chiffrer / Déchiffrer : avec une clé = action autorisée
- Décrypter : sans la clé = action non-autorisée

Cryptographie vs Stéganographie

- Etymologie du mot sténographie : mot issu du grec ; Stéganô signifiant Je couvre et Graphô signifiant J'écris
- La stéganographie est l'art de la dissimulation
- Présent chez les Grecs (485 an. J.C.)

Cryptologie vs Sécurité

La sécurité traite de la sécurisation de dispositifs (mise en oeuvre d'algorithmes cryptographiques, implémentation, gestion des droits d'accès, sécurité physique, . . .). Elle considère les primitives cryptographiques comme "parfaites".

La cryptologie n'est pas la sécurité, mais il n'y a pas de sécrurité sans cryptologie.

Une chaîne n'est jamais plus solide que son maillon le plus faible $\rightarrow$ éviter les systèmes trop complexes

Deuxième partie II

Age artisanal et technique de la crytographie

Plan de la seconde partie

L'âge artisanal de la cryptologie

Egyptiens (1900 av. J.C) : changement de mots et parties de documents relatifs aux constructions des Pharaons.

Scytale lacédémonienne : utilisée par les Grecs du Xème au VIIème siècle avant J.C.

L'âge artisanal (suite)

Carré de Polybe (125-200 av. J.C) : à l'origine pour la transmission de données (comme le morse)

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

L'âge artisanal (suite)

Substitution simple ou monoalphabétique (César) : A chaque lettre de l'alphabet, on associe une autre lettre (permutation). Soit $\mathcal{A} = \{a_1, \cdots, a_n\}$ un alphabet quelconque.

- Soit $\pi : \mathcal{A} \to \mathcal{A}$ une permutation (clé secrète).
- L'opération de chiffrement d'un message $m = m_1|m_2|m_3|\cdots|m_h$, où $m_i \in \mathcal{A}$ pour $h = 1 \cdots h$ est donnée par :

$$c = E_\pi(m) = \pi(m_1)|\pi(m_2)|\cdots|\pi(m_h)\,.$$

- L'opération de déchiffrement du message $c = c_1|c_2|\cdots|c_h$ est donnée par :

$$D_\pi(c) = \pi^{-1}(c_1)|\pi^{-1}(c_2)|\cdots|\pi^{-1}(c_h)\,.$$

L'âge artisanal (suite)

Exemple d'un système de chiffrement par substitution monoalphabétique.

1.
   - Texte clair : UNPREMIEREXEMPLEDECHIFFREMENT
   - La permutation est définie par : Exercice ;-)
   - Texte chiffré est : KBFQVTZQVAVTFPVYVREZOOQVTVBM
2. Décalage de l'alphabet (la clé secrète est la décalage). Pour un décalage de 3 vers la droite, ce système est appelé le *chiffre de César*. Par exemple, le mot "CESAR" est chiffré en "FHVDU".

L'âge artisanal (suite)

Al-Kindi (IXème ap. J.C.) : Analyse fréquentielle (cryptanalyse de la substitution simple).

Principe de l'analyse fréquentielle : fréquence des lettres non uniforme dans un texte (fonction de la langue).

Par exemple, en français : f_E=14,715%, f_S=7,948, $f_A = 7,636$ etc.
Associer la lettre de fréquence maximale dans le texte chiffré à E, la lettre de seconde fréquence maximale à S etc.

L'âge artisanal (suite)

Alberti (1466 ap. J.C.) : Substituation polyalphabétique, un disque représentant la permutation (+changement du décalage fréquemment). Surchiffrement codique.

Soit $\mathcal{A} = \{a_1, \cdots, a_n\}$ un alphabet et soit $(\pi_1, \cdots, \pi_t)$ des permutations de $\mathcal{A}$ (clé secrète). quelconque.

- L'opération de chiffrement d'un message $m = m_1|m_2|m_3|\cdots|m_t$, où $m_i \in \mathcal{A}$ pour $h = 1 \cdots t$ est donnée par :
$$c = E_\pi(m) = \pi_1(m_1)|\pi_2(m_2)|\cdots|\pi_t(m_t)\,.$$
- L'opération de déchiffrement du message $c = c_1|c_2|\cdots|c_t$ est donnée par :
$$D_\pi(c) = \pi_1^{-1}(c_1)|\pi_2^{-1}(c_2)|\cdots|\pi_t^{-1}(c_t)\,.$$

L'âge artisanal (suite)

Giovanni Battista Della Porta (1553-1563 ap. J.C.)
Classification des méthodes de chiffrement ; substitution et transposition

Chiffrement par transposition : Soit $\mathcal{A}$ un alphabet.

- Soit $\pi : \{1, 2, \ldots, t\} \to \{1, 2, \ldots, t\}$ une permutation (clé secrète).
- L'opération de chiffrement d'un message $m = m_1|m_2|m_3|\cdots|m_t$, où $m_i \in \mathcal{A}$ pour $h = 1 \cdots t$ est :

$$c = E_\pi(m) = c_{\pi(1)}|c_{\pi(2)}|\cdots|c_{\pi(t)}\,.$$

- L'opération de déchiffrement du message $c = c_1|\cdots|c_t$ est :

$$D_\pi(c) = m_{\pi^{-1}(1)}|m_{\pi^{-1}(2)}|\cdots|m_{\pi^{-1}(t)}\,.$$

L'âge artisanal (suite)

Blaise de Vigénère (1586 ap. J.C) : substitution polyalphabétique (utilise plusieurs chiffre de César).

Charles Babbage (1854) casse le chiffre de Vigenère ; "extension" de l'analyse fréquentielle : indice de coincidences.

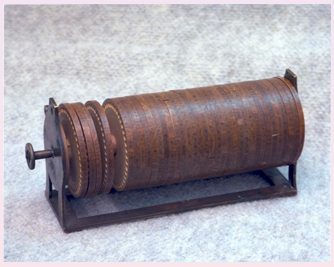
L'âge artisanal (suite)

Exemple : Le système de Vigenère ($\mathbb{XVI}$ème siècle).
Soit $\mathcal{A}$ un alphabet muni d'un ordre (p.ex. A, B, C, D, . . .).

- clé : mot clé de t caractéres qui spécifie le décalage à effectuer à chaque lettre d'un bloc de clair de t lettres. Exemple : CODE.
- Le clair : CESYSTEMEESTPEUSUR.
- Le chiffré correspondant : ESVCUHHQGSVXRSXWWF.

L'âge artisanal (suite)

Cylindre chiffrant (1790 ap. J.C.) : Thomas Jefferson.



L'âge technique

Dans la revue "Cryptographie militaire" (1883), le hollandais Auguste Kerckhoffs énonce six principes dont le plus important est :

> "Il [Le système de chiffrement] faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber dans les mains de l'ennemi"

CCL : Pas de sécurité par l'obscurité.

L'âge technique (suite)

Masque jetable (1917) : Vernam propose d'utiliser le chiffrement de Vigénère avec une clé

- purement aléatoire
- usage unique
- aussi longue que le message

Ce chiffrement est inconditionnellement sûr mais difficile à mettre en oeuvre.

L'âge technique (suite)

Description du système de Vernam.

- Opération de chiffrement : Pour chiffrer le message $m = m_1|m_2|\cdots|m_n$ où $m_i \in (\mathbb{Z}_2, +)$, on choisit une clé $k = k_1|k_2|\cdots|k_n$ où $k_i \in (\mathbb{Z}_2, +)$ (qui est supposé transmise au correspondant). Le chiffré est calculé par :

$$c = m_1 + k_1|m_2 + k_2|\cdots|m_n + k_n$$

- Opération de déchiffrement : Le clair est obtenu à partir de $c = c_1|c_2|\cdots|c_n$ où $c_i \in (\mathbb{Z}_2, +)$ par :

$$m = c_1 + k_1|c_2 + k_2|\cdots|c_n + k_n$$

Remarque : Opération VENONA.

L'âge technique (suite)

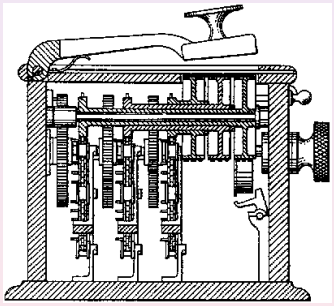
Enigma (1919) :

- Développé par l'allemand Arthur Scherbius.
- Version électro-méchanique des idées d'Alberti.
- Cassée par le mathématicien polonais Marian Rejewski (1933).
- Rôle important durant la seconde guerre mondiale (autre version cassée par les anglais).

L'âge technique (suite)

Chiffrement de Hill (1929) : Chiffrement (electro ?)-mécanique inventé par Lester S. Hill.

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$$



Remarque : les opérations sont faites dans l'anneau $\mathbb{Z}_{26}$

Définition de probabilité

Définition

Soit Ω un ensemble fini et $\mathcal{P}(\Omega)$ l'ensemble des parties de Ω. Une probabilité est une application $P : \mathcal{P}(\Omega) \to [0, 1]$ telle que :

- $P(\Omega) = 1$,
- $0 \leq P(A) \leq 1$ *pour tout* $A \in \mathcal{P}(\Omega)$,
- *Si* A_i *avec* $i \in I$ *sont des ensembles disjoints* ($A_i \cap A_j = \emptyset$ *si* $i \neq j$) *alors* $P(\cup_{i\in I} A_i) = \sum_{i\in I} P(A_i)$.

Remarque :

- $(\Omega, \mathcal{P}(\Omega), P)$ est appelé espace probabilisé.
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Définition de probabilité conditionnelle et propriété

Définition

Soit $(\Omega, \mathcal{P}(\Omega), P)$ un espace probabilisé (Ω est un ensemble fini). Soit $A, B \in \mathcal{P}(\Omega)$ deux évènements tels que $P(B) \neq 0$. La probabilité conditionnelle de A sachant B est définie par :

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}.$$

Théorème

Soit $(\Omega, \mathcal{P}(\Omega), P)$ un espace probabilisé (Ω est un ensemble fini) et $A, B \in \mathcal{P}(\Omega)$.

$$P(A \mid B) \cdot P(B) = P(B \mid A) \cdot P(A).$$

Remarque : $P(A \mid B)$, $P(A)$ et $P(B) \Rightarrow P(B \mid A)$.

Définition de probabilité conditionnelle et propriété

Théorème

Soit $(\Omega, \mathcal{P}(\Omega), P)$ un espace probabilisé (Ω est un ensemble fini). Soit $(B_i)_{i \in I}$ une partition de Ω. Alors, pour tout $A \in \mathcal{P}(\Omega)$,

$$P(A) = \sum_{i \in I} P(A \mid B_i) \cdot P(B_i).$$

Indépendance stochastique

Définition

Soit $(\Omega, \mathcal{P}(\Omega), P)$ un espace probabilisé (Ω est un ensemble fini). Deux évènements $A, B \in \mathcal{P}(\Omega)$ sont dits indépendants si et seulement si

$$P(A \cap B) = P(A) \cdot P(B)\,.$$

Définition de variable aléatoire

Définition

Une variable aléatoire est une application $X : \Omega \to \mathbb{R}$.

La probabilité de l'évènement $\{X = x\}$, notée $P(X = x)$, est $P(w \in \Omega \mid X(w) = x)$ avec $x \in \mathbb{R}$.

Remarque : On peut transposer tous les résultats précédents aux évènements $\{X = x\}$ ou $\{X \in B\}$ où B est un sous-ensemble de $\mathbb{R}$ (à mieux préciser !).

L'âge technique (suite)

Shannon (1949) (américain, père de la théorie de l'information),

"Mesurer la sécurité, c'est mesurer de l'information" [1]

- Notion de diffusion (// transposition)
- Notion de confusion (// substitution)
- Notion entropie,information mutuelle
- Chiffrement parfait : taille de la clé supérieure ou égale au message (ex. Vernam)

1. "Communication Theory of Secrecy Systems" publié en 1949 mais datant de 1945

L'âge technique (suite) : Diffusion

Diffusion : Celle-ci traite de la relation de dépendance entre les bits de sortie du chiffrement et les bits d'entrée.

Idéalement, on souhaite que l'algorithme de chiffrement soit tel que la modification de peu de bits d'entrée engendre le changement de chaque bit de sortie avec une probabilité $1/2$. Cette propriété porte le nom de critère de propagation .

Moyen d'y parvenir : utilisation de la transposition ou plus généralement d'applications linéaires (admis) .

L'âge technique (suite) : Confusion

Confusion : Celle-ci consiste à rendre la relation entre la clé et les textes chiffrés aussi complexe que possible . En tant que système d'équation en les variables de bits de clé, $E_K(m) = c$ doit être compliqué (haut degré algébrique p.ex).

Moyen d'y parvenir : utilisation de la substitution (fonctions non-linéaires)

L'âge technique (suite) : Principe de conception

Conclusion : La conception des algorithmes de chiffrement par bloc doit être basée selon Shannon (et d'autres personnes précédemment) sur la composition de ces deux principes.

Les critères sur le type de substitution et de transposition ont évolué au cours du développement du domaine .

Notions de théorie de l'information : Shannon (définition de l'entropie)

Définition

L'entropie d'une variable aléatoire X prenant chaque valeur x_i avec $i = 1...n$ avec une probabilité non-nulle $P(X = x_i) = p_i$ est définie par :

$$H(X) = -\sum_{i=1}^{n} p_i \cdot log_2(p_i)\,.$$

L'unité de l'entropie est le bit.

Notions de théorie de l'information : propriétés de l'entropie)

Théorème

Considérons une variable aléatoire X prenant chaque valeur x_i avec $i = 1...n$ avec une probabilité non-nulle $P(X = x_i) = p_i$. Alors

$$0 \leq H(X) \leq log_2(n)$$

De plus,

- *$H(X) = log_2(n)$ si et seulement si $p_i = \frac{1}{n}$ pour tout $i \in \{1, \cdots, n\}$ (distribution uniforme),*
- *$H(X) = 0$ si et seulement si $n = 1$ et $p_1 = 1$ (dist. dégénérée)*

Remarque : L'entropie est une mesure d'uniformité : au plus on se rapproche de la distribution uniforme (incertitude importante) au plus elle est grande.

Notions de théorie de l'information : entropie conditionnelle

Soient $X, Y : \Omega \to \mathbb{R}$ deux variables aléatoires. Les différentes valeurs en lesquels la probabilités de Y est non-nulle est l'ensembles S_Y.

Pour tout $y \in S_Y$ fixé, considérons la distribution de X connaissant Y, i.e. $P(X = x \mid Y = y)$. Dénotons par $S_{X|y}$ l'ensemble des valeurs en lesquels cette distribution est non-nulles.

Appliquons la fonction entropie à cette distribution, i.e.

$$H(X \mid Y = y) = - \sum_{x \in S_{X|y}} P(X = x \mid Y = y) \cdot log_2(P(X = x \mid Y = y))$$

Notions de théorie de l'information : entropie conditionnelle

On définit l'entropie conditionnelle par rapport à Y en prenant l'espérance de cette v.a.

Définition

Soient les variables aléatoires $X, Y : \Omega \to \mathbb{R}$. L'entropie conditionnelle de X par rapport à Y est définie par :

$$H(X \mid Y) = \sum_{y \in S_Y} H(X \mid Y = y) \cdot P(Y = y)\,.$$

où l'ensemble S_Y est défini précédemment.

Notions de théorie de l'information : entropie conditionnelle et information mutuelle

Théorème

$$H(X \mid Y) \leq H(X)$$

et $H(X \mid Y) = H(X)$ si et seulement si X est stochastiquement indépendant de Y.

Définition

L'information mutuelle entre les v.a's X et Y est définie par

$$I(X, Y) = H(X) - H(X \mid Y).$$

Cette quantité est toujours positive et représente la perte d'incertitude (=gain d'information) sur X apportée par la connaissance de Y.

Chiffrement parfait

Contexte :

Objectif : On souhaite que le chiffré c ne donne aucune information sur le message m.

Définition

On dit qu'un système de chiffrement est parfait si $I(M \mid C) = 0$.

Théorème

(Shannon, 1949). Le chiffrement de Vernam est parfait.

Chiffrement parfait

Théorème

(Shannon, 1949). Pour un système de chiffrement parfait, l'entropie sur la clé est supérieure à celle sur le message $H(K) \geq H(M)$

Remarque : cela signifie en particulier que si la distribution uniforme est appliquée sur l'espace des clés et des messages, la longueur de la clé est toujours supérieure à celle du message (Notons que notre contexte impose de changer la clé pour chaque message).

Troisième partie III

Etablissement des enjeux de la cryptographie moderne

Plan de la troisième partie

Avènement des ordinateurs

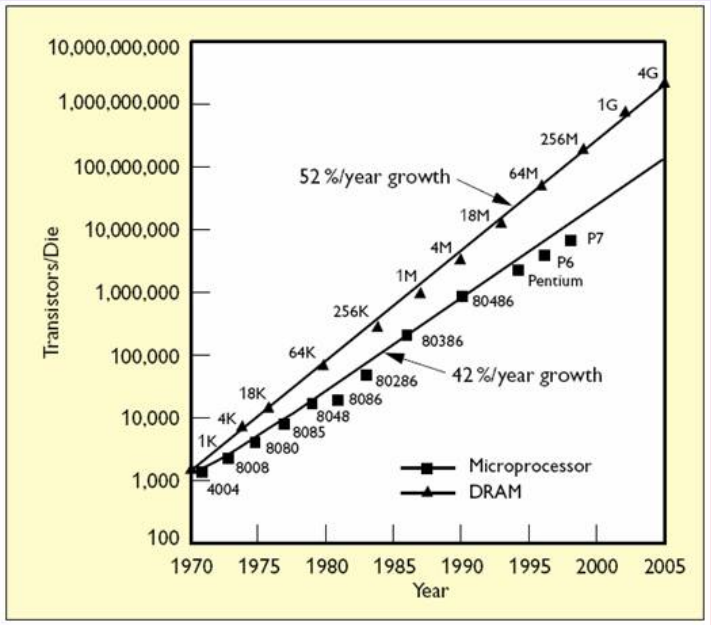
- Invention du transistor en 1947 (laboratoires Bell, John Bardeen, Walter Brattain et William Schockley). Prix Nobel pour leur invention en 1956.
- Industrialisation du transistor dans les années 1960.
- Modification profonde du monde industrielle suite à cette découverte (peu de changement depuis lors).

Loi de Moore

Loi de Moore (1965 et 1975) : densité des transistors d'un processeur double tous les 2 ans (observé entre 1971 et 2001). Moore (cofondateur d'Intel) pense que cela ne sera plus vrai dans dix à quinze ans.

Fausse loi de Moore : "quelque chose" double tous les dix-huit mois, cette chose étant la *puissance*, la *capacité* ou la *vitesse* (pas énoncé par Moore et pas sensé)

Loi de Moore (suite)



Avènement des réseaux informatiques

- 1966 : projet de création d'un réseau informatique délocalisé, reliant les universités contrat avec la DARPA (Defense Advanced Research Projects Agency).
- 1969 : le réseaux de transfert de paquets est opérationnel. Il est baptisé "ARPANET" (acronyme anglais de "Advanced Research Projects Agency Network"). Les deux premiers noeuds ont été l'université de Stanford et UCLA.
- 1972 : démonstration officielle.
- 1974 : TCP/IP (Transmission Control Protocol et Internet Protocol) est créé pour uniformiser le réseau (encore d'actualité).
- 1980 : division du réseau ARPANET en un réseau militaire et universitaire.

Du monde militaire au monde civil

Grâce à son développement, la technologie va se démocratiser et entrer dans le monde de l'entreprise. La sécurité et la cryptographie vont désormais intéresser le monde civil.

- Fin de la seconde guerre mondiale : peu de choses dans le monde civil (uniquement dans le monde militaire et diplomatique)
- 1967 : "Codes breakers" (David Kahn)
- 1971 : l'algorithme de chiffrement (par bloc) Lucifer fut développé par Feistel *et al.* pour le compte d'IBM. Version DTD-1 utilisée pour le e-banking durant les années 70.

Différents types d'attaques

1. **Criminelles :** Fraude (obtention de numéros de cartes), escroquerie (phishing), attaques destructrices (effacer un disque), vol de propriété intelectuelle, vol d'identité, vol de marques,
2. **Violation de la vie privée :** collecte d'information privée (cela peut être légal : ex. Facebook), surveillance (légal ou pas)
3. **Publicité :** attaques en vue d'être connu, attaque "denial of service" (empêcher un service de fonctionner)

Qui sont les attaquants ?

1. Hacker's (programme "exploit")
2. Criminels isolés
3. Interne malicieux
4. Espionnage industriel
5. Crime organisé
6. Terroristes
7. Services d'intelligence

Besoins en sécurité ?

1. Vie privée
2. Authentification (données et personnes)
3. Intégrité
4. anonymité (commerciale, médicale)
5. Monnaie et vote électronique
6. Solutions proactives
7. Multiniveau
8. Audit

Cryptographie au sein d'un réseau ?

Dans le cas de la confidentialité par exemple, les solutions basées sur la cryptographie d'hier nécessitent que chacun dispose de $n-1$ clés (groupe de n personnes).

Cela signifie $C_n^2 = (n-1)n/2$ paires de clés différentes.

Difficulté de gestion ! !

Cryptographie au sein d'un réseau ? (suite)

On va donc devoir considérer un cadre solution additionnel à celui de la cryptographie d'hier :

Hypothèses :

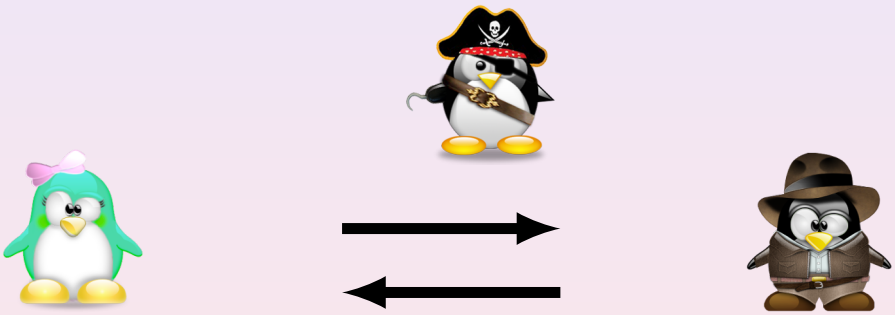
- De nombreux intervenants en présence d'un pirate.
- Les intervenants ne peuvent pas toujours se rencontrer avant l'ensemble des échanges afin de se mettre d'accord sur un ensemble de paramètres.

Enjeux de la cryptographie moderne

1. Confidentialité : personne ne doit pouvoir prendre connaissance du contenu des données
2. Authenticité :
   - des données : personne ne doit pouvoir contrefaire l'origine des données
   - des personnes : être capable de prouver à quelqu'un qu'on est bien la personne que l'on prétend être
3. Intégrité : service permettant de vérifier que personne n'a modifié les données
4. Non-répudiation : personne ne doit pouvoir nier avoir commis une action

Confidentialité

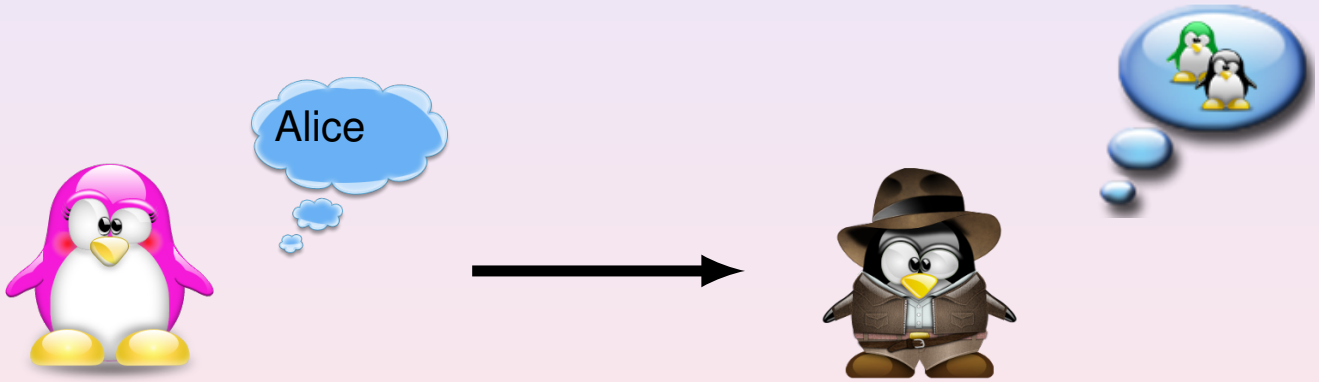
S'assurer du caractère secret de l'information



Stockage de données sécurisé

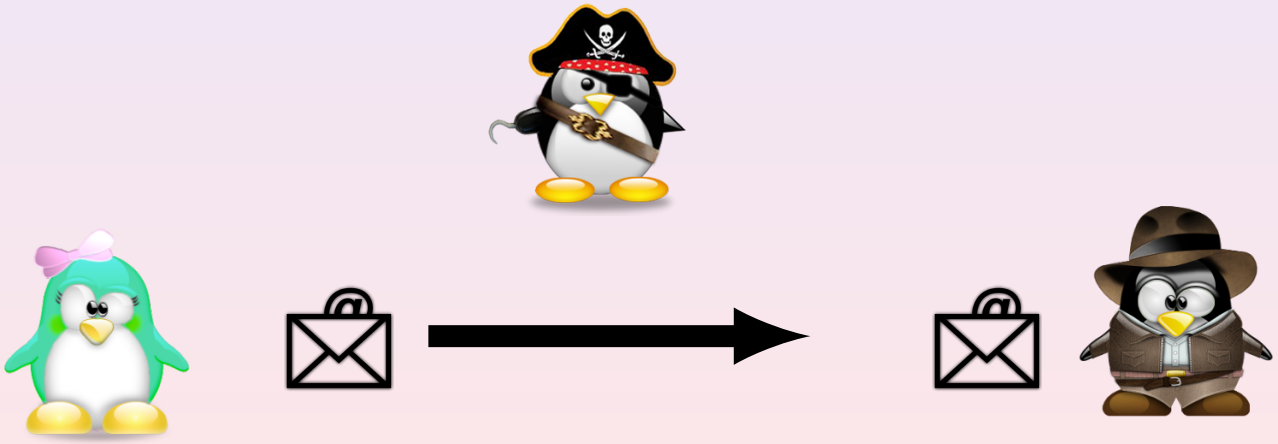
Authenticité

Des personnes : être capable de vérifier qu'une personne est bien celle qu'elle prétend être

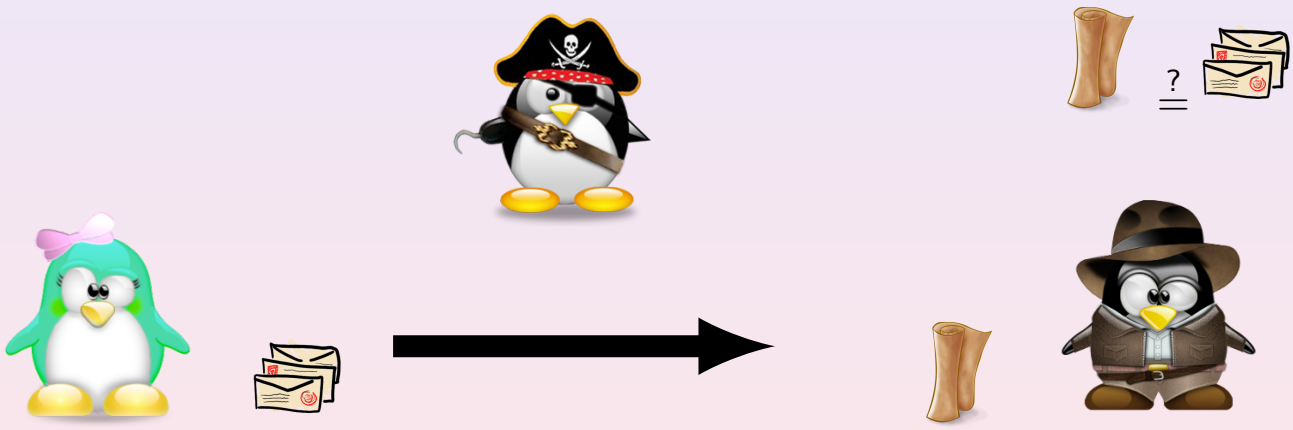


Authenticité

Des données : être capable de vérifier que des données proviennent de l'émetteur



Intégrité



Non-répudiation

Etre capable de prouver que quelqu'un a commis une action

Quatrième partie IV

Conclusion

Conclusion

Deux types de modèles :

Cas où les intervenants peuvent se rencontrer au préalable

Ce modèle provient de la cryptographie d'hier. Dans ce cas les intervenants disposent d'une valeur secrète commune et ce type de cryptographie est donc dit "symétrique". La conception de ces algorithmes nécessite l'utilisation de mathématiques avancées (probabilité, algèbre).

Conclusion (suite)

Cas où les intervenants **ne** peuvent **pas** se rencontrer au préalable

Ce modèle fût introduit récemment (années 70) étant donné l'avènement des réseaux informatiques. Dans ce modèle, les intervenants disposent de valeurs secrètes différentes mais liées et ce type de cryptographie est donc dit "asymétrique". La conception de ces algorithmes nécessite l'utilisation de mathématiques avancées.

Remarque : Etant donné les nouvelles technologies (circuits, ordinateurs), l'évaluation des algorithme est plus rapide mais les attaques sont aussi potentiellement plus puissantes $\rightarrow$ une modélisation mathématique plus poussée est nécessaire !

Source des images :

- png factory
- tux factory
- wikipedia