

Modèles pour la sécurité

Jean-Louis Roch

ESIMAG - ISI



25 octobre 2007

Organisation des 4 séances

- ① Modèles d'attaques - Sécurité inconditionnelle, prouvée, sémantique
- ② Chiffrement symétrique inconditionnellement sûrs
- ③ Sécurité prouvée d'un chiffrement public (RSA)
- ④ Générateur aléatoire cryptographiquement sûr et padding
- ⑤ Fonctions de hachage cryptographiquement sûrs
- ⑥ Protocoles à divulgation nulle de connaissance (zero-knowledge)

Ref : *Théorie des Codes : compression, cryptage, compression.*
JG Dumas, JL Roch, E Tannier, S Varrette. Dunod.

- ① Introduction : attack models and security properties**
- ② Security definitions and proofs - Perfect secrecy
- ③ Elementary notions in probability theory
- ④ Shannon' theorem on perfect secrecy

Security : what cryptography should provide

CAIN

- Confidentiality
- Authentication
- Integrity
- Non-repudiation

Kerckhoffs' principle [1883]

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

What a cryptographic protocol should provide :

- "real-time" encoding/decoding : cost= $\Theta(\text{message size})$
- "impossibility" for an attacker to decrypt an encrypted message without knowing the secret decoding function

Attack models : COA / KPA / CPA / CCA (1/2)

COA : Ciphertext-Only Attack

the attacker is assumed to have access only to a set of ciphertexts

Eg : *vulnerabilities to COA :*

- *WEP : bad design ;*
- *DES : too small key space*

KOA : Known-Plaintext Attack

the attacker has samples of both the plaintext and its encrypted version ; he uses them to get the secret key.

Eg : *vulnerabilities to KOA : encrypted ZIP archive : knowing only one unencrypted file from the archive is enough to calculate the key*

CPA : Chosen-Plaintext Attack

the attacker chooses a plaintext and can crypt it to obtain the corresponding ciphertexts ; i.e.

he has access to an encryption machine.

Eg : *vulnerabilities to COA : dictionary attack on Unix passwd file.*
Crack, John the Ripper, L0phtCrack, Cain&Abel, ...

CCA : Chosen-Ciphertext Attack

the attacker chooses a ciphertext and can decrypt without knowing the key.

He has access to a decryption machine (oracle).

→ Important for smart cards designers, since the attacker has full control on the device !

Eg : *vulnerabilities to CCA : ElGamal, early versions of RSA in SSL, ...*

- ① Introduction : attack models and security properties
- ② **Security definitions and proofs - Perfect secrecy**
- ③ Elementary notions in probability theory
- ④ Shannon' theorem on perfect secrecy

Security definitions. A cryptosystem is

Computationally secure :

if any successful attack requires at least N operations, with N large
eg $10^{120} \simeq 2^{400}$.

Provable secure :

if any attack exists, a known hard problem could be efficiently solved.
[Proof : **reduction**, complexity, P, NP]

Semantic secure – for asymmetric cryptosystem – :

knowing the public key and a ciphertext (COA), it must be infeasible for a **computationally-bounded** adversary to derive significant information about the plaintext

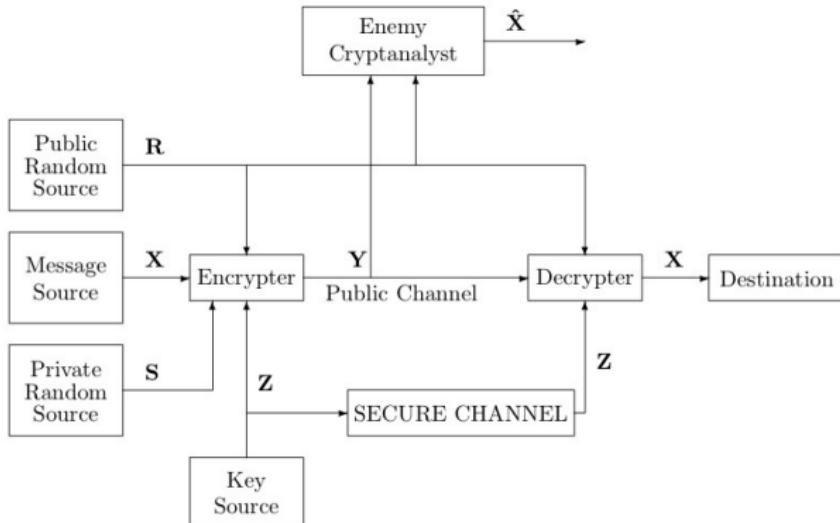
NB equivalent to the property of *ciphertext indistinguishability* [Blum, Micali]

Unconditionally secure : (or perfect secrecy)

cannot be broken, even by a **computationally-unbounded** attack

↪ "Information Theory" [Shannon]

Model of a symmetric cryptosystem



Shannon model

- perfect secrecy : i.e., informally,
the knowledge of Y gives no information on X
- ↵ definition : “Information Theory”

- ① Introduction : attack models and security properties
- ② Security definitions and proofs - Perfect secrecy
- ③ **Elementary notions in probability theory**
- ④ Shannon' theorem on perfect secrecy

Discrete Random Variable (1/2)

- **Sample space** S : finite set whose elements are called "elementary events"
Eg : can be viewed as a possible outcome of an experiment
- an **event** is a subset of S .
 \emptyset = the *null* event S = the *certain* event
- events A and B are **mutually exclusive** iff $A \cap B = \emptyset$
- **Probability distribution**
a function $\Pr : X \subset S \mapsto [0, 1]$ satisfying probability axioms :
 - ① \forall event $A : \Pr(A) \geq 0$;
 - ② if A and B mutually exclusive : $\Pr(A \cup B) = \Pr(A) + \Pr(B)$
 - ③ $\Pr(S) = 1$

Discrete Random Variable (2/2)

Definition : Discrete Random Variable

a function X from a finite space S to the real numbers.

↪ *quantity whose values are random*

For a real number x , the event $X = x$ is $\{s \in S : X(s) = x\}$. Thus

$$\Pr(X = x) = \sum_{s \in S : X(s) = x} \Pr(s)$$



Experiment = rolling a pair of fair 6-sided dice

- Random variable X : the maximum of the two values
- $\Pr(X = 3) = \frac{5}{36}$

Conditional probability and independence

Def : Conditional property of an event A given another event B :

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$$

Def : Two events A and B are **independent** iff

$$\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$$

So, if $\Pr(B) \neq 0$, A and B independent $\iff \Pr(A|B) = \Pr(A)$

Bayes's theorem

From definition,

$$\Pr(A \cap B) = \Pr(B \cap A) = \Pr(B) \Pr(A|B) = \Pr(A) \Pr(B|A).$$

This, if $\Pr(B) \neq 0$, we have :

$$\Pr(A|B) = \frac{\Pr(A) \Pr(B|A)}{\Pr(B)}$$

Birthday paradox

Birthday paradox

Let E be a set of n elements.

If $\lceil 1.18\sqrt{n} \rceil$ elements are randomly chosen in E , then the probability of a collision is larger than 50%.

Example

- There are $\simeq 365$ days in a year, so 365 birthdays possible.
- In a group of $k = 1.18\sqrt{365} \simeq 22.5$ peoples, the probability that two persons have the same birthday is $\geq \frac{1}{2}$!!

Many applications in cryptography

block cipher (2-DES) ; collisions for hash functions, ...

- ① Introduction : attack models and security properties
- ② Model of a symmetric cryptosystem
- ③ Elementary notions in probability theory
- ④ **Information theory - Shannon' theorem on perfect secrecy**

Information and entropy

Shannon's measure of information

- Hartley's measure of information : $I(X) = \log_2 \frac{1}{p_i}$ bit (logon)
- Def : entropy $H(X)$ (or uncertainty) of a disc. rand. var. X :

$$H(X) = - \sum_{x \in \text{Supp}(X)} \Pr(X = x) \cdot \log_2 \Pr(X = x)$$

i.e. the "average Hartley information".

Basic properties of entropy

- Let $n = \text{Card}(\text{Sample space})$; then $H(X) \leq \log_2 n$
The entropy is maximum for the uniform probability distribution Gibbs'lemma
- $H(X|Y) \leq H(X) + H(Y)$
- $H(XY|Z) = H(Y|Z) + H(X|YZ)$
- $H(X|Y) \leq H(XZ|Y)$

Characterization of perfect secrecy

The knowledge of the ciphertext Y brings no additional information on the plaintext X , i.e.

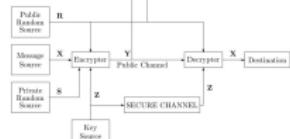
$$H(X|Y) = H(X)$$

Theorem (Shannon's theorem on perfect secrecy)

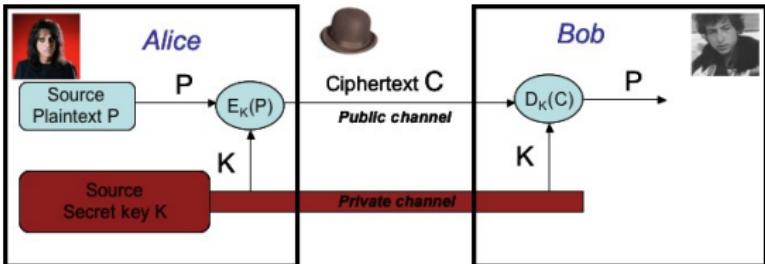
If a symmetric cryptosystem ensures perfect secrecy, then the entropy of the secret shared key Z is larger than the one of the plaintext X .

If $H(X|Y) = H(X)$ then we have : $H(Z) \geq H(X)$

Unconditional security of a symmetric cryptosystem



General model



Simplified model

Definition : Unconditional security or Perfect secrecy

The symmetric cipher is **unconditionally secure** iff $H(P|C) = H(P)$

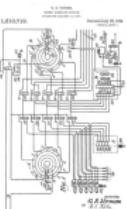
i.e. the cryptanalyst's a-posteriori probability distribution of the plaintext, after having seen the ciphertext, is identical to its a-priori distribution.

Shannon's theorem : necessary condition, lower bound on K

In any unconditionally secure cryptosystem : $H(K) \geq H(P)$.

Proof : $H(P) = H(P|C) \leq H((P, K)|C) = H(K|C) + H(P|(K, C)) = H(K|C) \leq H(K)$

Vernam's cipher : unconditionally secure cryptosystem



Symmetric cipher of a bit stream :

- let \oplus = boolean xor; let $n = |P|$.
- for $i = 1, \dots, n$: $C_i = P_i \oplus K_i$

Vernam's patent, 1917

OTP : One-Time Pad [AT&T Bell labs]

NB : size of the (boolean) key K = size of the (boolean) plaintext P .

Theorem : Vernam's cipher is unconditionally secure

Proof :

Application One-time pad

- Unbreakable if used properly. A one-time pad must be **truly random data** and must be **kept secure** in order to be unbreakable.
- intensively used for diplomatic communications security in the 20th century. E.g. telex line Moscow-Washington : keys were generated by hardware random bit stream generators and distributed via trusted couriers.
- In the 1940s, the (Soviet Union) KGB used recycled one-time pads, leading to the success of the NSA code-breakers of the project VENONA
[<http://www.nsa.gov/venona/>]



- E_K, D_K one-way mapping (bijective) $\{0, 1\}^n \rightarrow \{0, 1\}^n$
- block encryption : S-box + rounds + key expansion
each round= composition of permutation and substitution
 - DES : block size=64 bits ; key size = 56 bits
 - AES : block size=128 ; key size= 128, 192 or 256
- chaining mode

Conclusion

- It is possible to provide unconditional security, but keys are too long for a practical use
- tradeoff : block cipher
- Next lecture : asymmetric cryptography and provable security