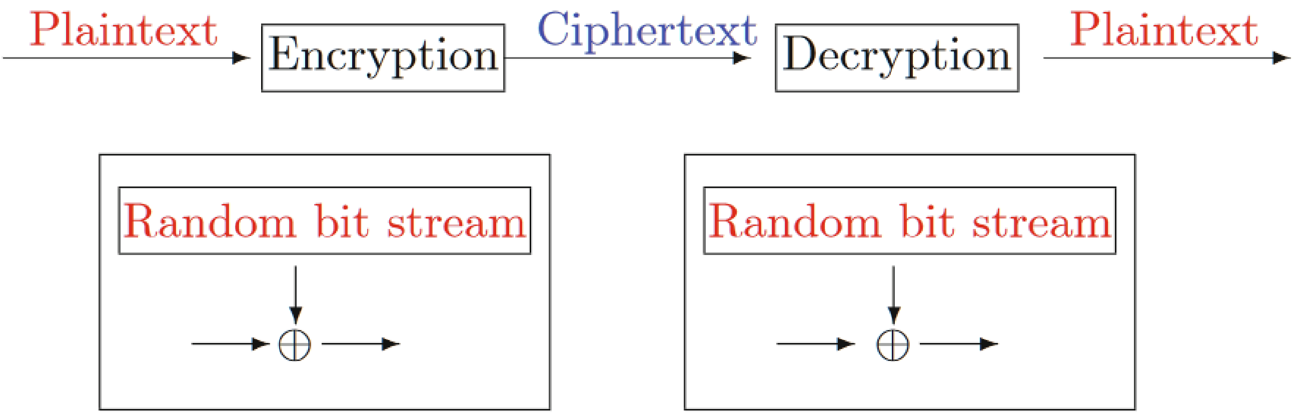
Stream Ciphers

Stream Ciphers



Definition - cipher
A Cipher is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ and is a pair of efficient algorithms (E, D)

- E is randomized, D is deterministic
- $E : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$
- $D : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$
- has the **Corectness propriety**: $\forall m \in \mathcal{M}, k \in \mathcal{K} => D(k, (E(k, m))) = m$
- Is efficient
  - Polynomial time
  - In good time

Example One time pad
$E(k, m) = k \oplus m$
$D(k, c) = k \oplus c$
$D(k, E(k, c)) = k \oplus k \oplus m = m$

Perfect secrecy

A cipher (E, D) has perfect secrecy if

- for all $m_0, m_1 \in \mathcal{M}$, and all $c \in \mathcal{C}$
- we have $Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$

Intuition:

- All messages are **equaly** likely to be the ciphertext
- No adversary can learn something about the m from c

- No chosen cipher attack

Example:
OTP is perfectly secure

The bad news

- For (E, D) to have perfect secrecy => $|\mathcal{K}| > |\mathcal{M}|$
- So for each message we will need to send a key that is the same or bigger size => impractical
- If we already have a secure channel to communicate the key there is no use for the OTP
- Don't reuse the key

Semantic security

Stream ciphers

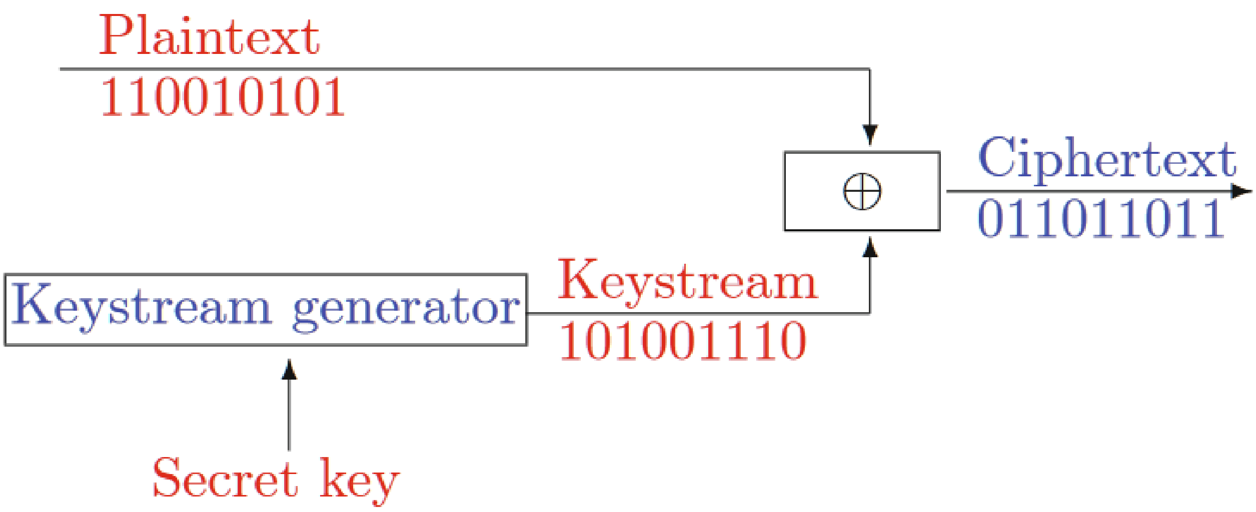


FIGURE 10.2. Stream ciphers

We use a seed to generate a key (Pseudorandom generator)

- We put a 128 seed into a function G that outputs a 2048 number
- $k = G(s)$ where s = seed

Let (E, D) be a cipher.

- $c = E(k, m) = E(G(s), m)$

Remark

- Stream ciphers cannot have perfect secrecy!
- We need a new definition for security
- PRG must be unpredictable

A PRG is predictable if given the first n-1 bits we can predict the next bits

PRG security

We want the PRG to be indistinguishable from the true random distribution
Let $A(x)$ be a **statistical test**

- 0 if the output is not random
- 1 if the output is random
- Examples
  - $|nr(0) - nr(1)| \leq 10 \cdot \sqrt{(n)}$ (nr of 0 - nr of 1)
  - $nr(00) \leq 10 \cdot \sqrt{(n)}$
  - longest sequence of 0

Let $G : K \longrightarrow \{0,1\}^n$ and define **Advantage** as:
$\text{Adv}(A, G) = |Pr[A(G(k)) = 1] - Pr[A(k) = 1]| \in [0,1]$

- If $\text{Adv} \rightarrow 1$ => A can distinguish from random
- If $\text{Adv} \rightarrow 0$ => A can't distinguish from random

Example:
Suppose

- $msb(G(k)) = 1$ for $2/3$ of $k \in K$
- $A(x) = 1 \iff msb(x) = 1$

Then

- $\text{Adv}(A, G) = |Pr[A(G(k)) = 1] - Pr[A(k) = 1]| = |2/3 - 1/2| = 1/6$

Definition - prg security
A PRG is secure if for all effiecient statistical tests A the $\text{Adv}(A, G)$ is negligible

Theorem

> If the genrator G is secure => a PRG based on it it's unpredictable

Theorem

> An unpredictable PRG is secure (Then the G is secure)

Definition - computantional indistinguishability
Let P_1, P_2 be two distrib over $\{0,1\}^n$
We say that P_1, P_2 are **computationally indisinguishable** if:

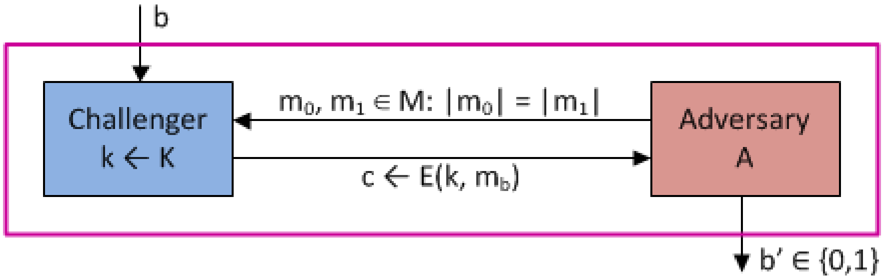
- $\forall$ efficient statistical tests A
- $|\underset{x \leftarrow P_1}{Pr}[A(x) = 1] - \underset{x \leftarrow P_2}{Pr}[A(x) = 1] < \epsilon$
- ϵ is negligible

Semantic security

https://www.youtube.com/watch?v=9MfeDP0fNDY

Intuition:

- Having the ciphertext does reveal a negligible amount about the original message / key
- An attacker that has the ciphertext must have the same information as one without it



Definition - semantic security

- Let $\mathcal{E} = (E, D)$ be a cipher
- Let $EXP(0)$, and $EXP(1)$ be two experiments
- An adversary A sends $m_0, m_1 \in M$ to the challenger
- The challenger sens an encryption of **one** of them ($EXP(0)$ or $EXP(1)$)
- The adversary must guess which one
- $W_b = \text{ event that } EXP(b) = 1$ = event that in $EXP(b)$ the Adversary outputs 1
- $\text{Adv}_{SS}(A, \mathcal{E}) = |PR[W_0] - Pr[W_1]| \in [0, 1]$
    - *intuition*: We look if the adversary behaves diferently if he is given one ciphertext or the other
    - If Adv is close to 1 => The adversary can distinguish between the encryptions

$\mathcal{E}$ is semantically secure if for all adversaries A

- $\text{Adv}_{SS}(A, \mathcal{E}) < \epsilon$

Stream ciphers are semantically secure

Theorem

> $G : K \longrightarrow \{0, 1\}^n$ is a secure PRG => the Stream cipher is semantically secure

More Resources

- https://en.wikipedia.org/wiki/Stream_cipher - wiki page
- https://www.youtube.com/watch?v=rAFNmO-4CIA - Another short explanation
- https://www.youtube.com/watch?v=W39KqX0ZTbU - Another long explanation
- http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf - Shannon security paper