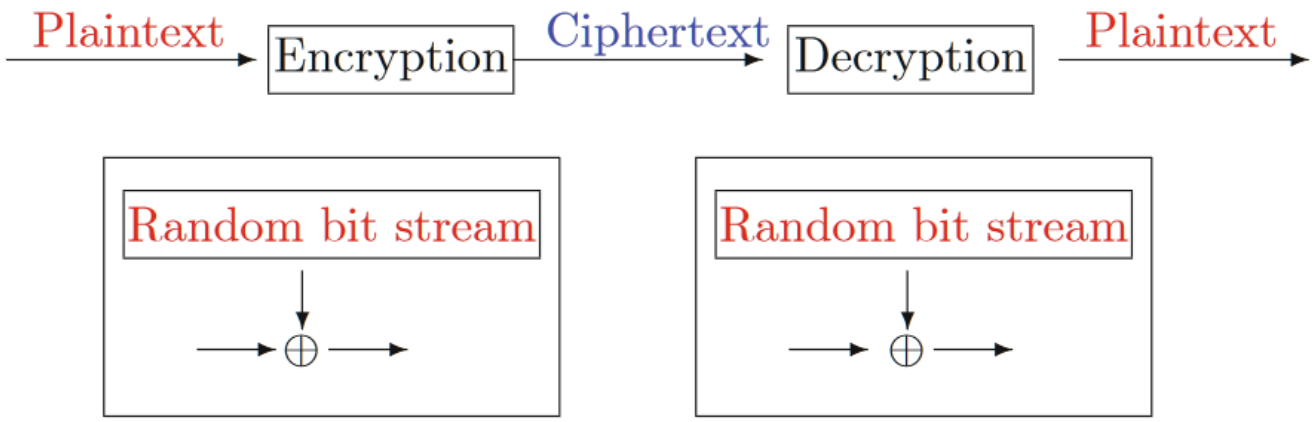
Stream Ciphers



Stream ciphers

The idea is to make our ciphertext as indistinguishable from random as possible. Since the message is fixed we want to generate the key in a smart way to make it as random as possible. We are using pseudorandom generators to generate the key and $\oplus$-ing it with the message like in the OTP setting.

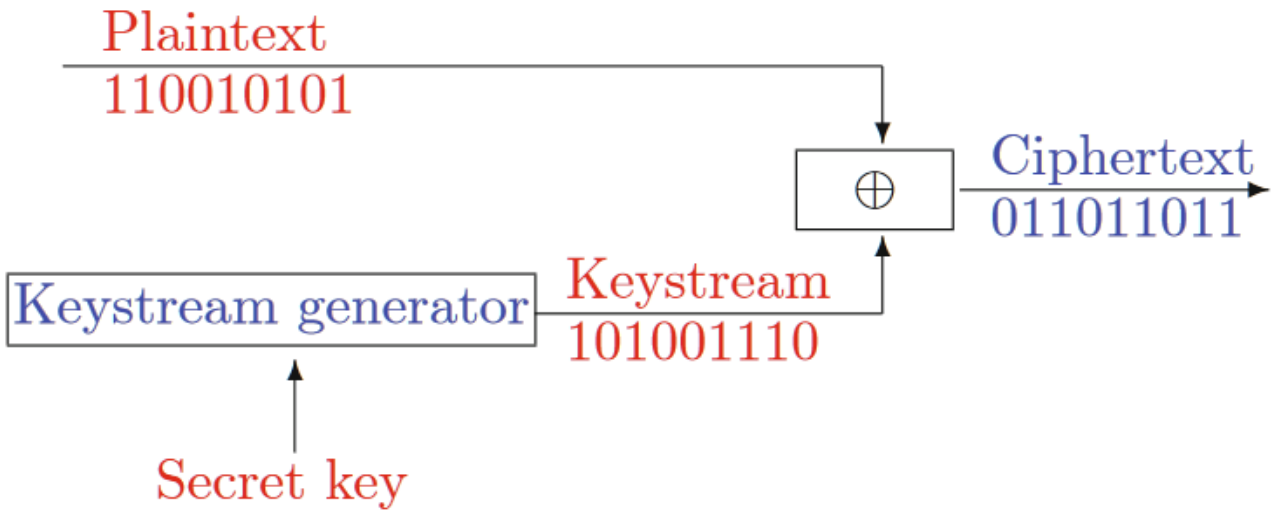


FIGURE 10.2. Stream ciphers

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.

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

Remark

- Stream ciphers cannot have perfect secrecy since $|\mathcal{M}| < |\mathcal{K}|$! 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:

$$\mathrm{Adv}(A, G) = |Pr[A(G(k)) = 1] - Pr[A(k) = 1]| \in [0, 1]$$

- If $\mathrm{Adv} \to 1 \Rightarrow A$ can distinguish from random
- If $\mathrm{Adv} \to 0 \Rightarrow A$ 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

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

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

Theorem
If the generator G is secure $\Rightarrow$ a PRG based on it is unpredictable

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

Theorem

> $G : K \to \{0,1\}^n$ 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