Stream ciphers

The One Time Pad

Symmetric Ciphers: definition

Def: a **cipher** defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

is a pair of "efficient" algs (***E***, ***D***) where

$E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, $D: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

s.t. $\forall m \in \mathcal{M}, k \in \mathcal{K}:$ $D(k, E(k,m)) = m$

- ***E*** is often randomized. ***D*** is always deterministic.

The One Time Pad (Vernam 1917)

First example of a "secure" cipher

$\mathcal{M} = \mathcal{C} = \{0,1\}^n$, $\mathcal{K} = \{0,1\}^n$

key = (random bit string as long the message)

The One Time Pad (Vernam 1917)

$c := E(k, m) = k \oplus m$

$D(k, c) = k \oplus c$

msg:	0	1	1	0	1	1	1	$\oplus$
key:	1	0	1	1	0	1	0	
CT:								

Indeed:

$D(k, E(k,m)) = D(k, k \oplus m) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$

You are given a message (m) and its OTP encryption (c).

Can you compute the OTP key from m and c ?

No, I cannot compute the key.

Yes, the key is $k = m \oplus c$.

I can only compute half the bits of the key.

Yes, the key is $k = m \oplus m$.

The One Time Pad (Vernam 1917)

Very fast enc/dec !!

… but long keys (as long as plaintext)

Is the OTP secure? What is a secure cipher?

What is a secure cipher?

Attacker's abilities: **CT only attack** (for now)

Possible security requirements:

attempt #1: **attacker cannot recover secret key**

$E(k,m)=m$ would be secure

attempt #2: **attacker cannot recover all of plaintext**

$E(k, m_0 \| m_1) = m_0 \| k \oplus m_1$ would be secure

Shannon's idea:

CT should reveal no "info" about PT

Information Theoretic Security
(Shannon 1949)

Def: A cipher (***E***, ***D***) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has **perfect secrecy** if

$\forall m_0, m_1 \in \mathcal{M}$ $(\text{len}(m_0) = \text{len}(m_1))$ and $\forall c \in \mathcal{C}$

$$\boxed{\Pr[E(k, m_0) = c] = \Pr[E(k, m_1) = c]}$$

where k is uniform in $\mathcal{K}$ $(k \xleftarrow{R} \mathcal{K})$

Information Theoretic Security

Def: A cipher (***E***, ***D***) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has **perfect secrecy** if

$\forall m_0, m_1 \in \mathcal{M}$ $(|m_0| = |m_1|)$ and $\forall c \in \mathcal{C}$

$$Pr[\, E(k, m_0) = c\,] = Pr[\, E(k, m_1) = c\,] \quad \text{where} \quad k \xleftarrow{R} \mathcal{K}$$

⟹ Given CT can't tell if msg is m_0 or m_1 (for all m_0, m_1)

⟹ most powerful adv. learns nothing about PT from CT

⟹ no CT only attack!! (but other attacks possible)

Lemma: OTP has perfect secrecy.

Proof:

$$\forall m, c: \quad \Pr_{k}\left[E(k,m) = c \right] = \frac{\#\text{keys } k \in \mathcal{K} \text{ s.t. } E(k,m)=c}{|\mathcal{K}|}$$

So: if $\forall m, c$: $\#\{k \in \mathcal{K} : E(k,m) = c\} = \text{const.}$

$\Longrightarrow$ cipher has perfect secrecy

Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.

How many OTP keys map $\boldsymbol{m}$ to $\boldsymbol{c}$?

None

1

2

Depends on $\boldsymbol{m}$

Lemma: OTP has perfect secrecy.

Proof:

For OTP: $\forall m, c:$ if $E(k,m) = c$

$\Longrightarrow k \oplus m = c \Longrightarrow k = m \oplus c$

$$\Longrightarrow \boxed{\#\{k \in \mathcal{K} : E(k,m) = c\} = 1}$$

$\Longrightarrow$ OTP has perfect secrecy ∎

The bad news …

Thm: perfect secrecy $\Rightarrow$ $|\mathcal{K}| \geq |\mathcal{M}|$

i.e. perfect secrecy $\Longrightarrow$ key-len $\geq$ msg-len

$\Longrightarrow$ hard to use in practice !!

End of Segment