One Time Pad

MSc in Information Security & Digital Forensics.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

What is a *Cipher?*

Symmetric Ciphers : Definition

A cipher defined over $(\mathcal{K},\mathcal{M},\mathcal{C})$

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

$$E: \mathcal{K} * \mathcal{M} \rightarrow \mathcal{C}, \qquad D: \mathcal{K} * \mathcal{C} \rightarrow \mathcal{M}$$

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

consistency equation

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

One Time Pad

First example of a 'secure' cipher (Vernam 1917)

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

key = (random bit string as long the message)

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

One Time *Pad*

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

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

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

One Time Pad

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 $\boxed{k = m \oplus c}$.
- I can only compute half the bits of the key.
- Yes, the key is $k = m \oplus m$.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

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?

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Def:

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

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

$$Pr\left[\, E(k, m_0) = c \,\right] = Pr\left[\, E(k, m_1) = c \,\right]$$

where $\quad k \leftarrow \mathcal{K}$

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Information Theoretic ***Security*** ***(Shannon 1949)***

- Given CT we can't tell if msg is m_0 or m_1 (For all m_0, m_1)
- Most powerful adversary learns nothing about PT from CT
- No CT only attack (but other attacks are possible)

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Lemma: OTP has perfect secrecy.

Proof:

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

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

= Cipher has perfect Secrecy

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Information Theoretic Security (Shannon 1949)

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 $\boldsymbol{m}$

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

The bad news

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

i.e. Perfect secrecy $\Rightarrow$ key length $\geq$ msg length

Hard to use in practice

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Thank You !

End of Section

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie