Introduction to Cryptology

2.2 - One Time Pad (OTP)

Federico Pintore

Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

One Time Pad (Vernam 1917 or $\sim$ 35 years earlier)

Fix an integer $n > 0$, and let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$.

One Time Pad (Vernam 1917 or $\sim$ 35 years earlier)

Fix an integer $n > 0$, and let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$.

- KeyGen(n) : it returns a uniformly random bit string k of length n, i.e. $k \in \mathcal{K}$.
- Enc(k, m) : it outputs the ciphertext $c = k \oplus m$.
- Dec(k, c) : it recovers the message computing $m = k \oplus c$.

One Time Pad (Vernam 1917 or $\sim$ 35 years earlier)

Fix an integer $n > 0$, and let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$.

- KeyGen(n) : it returns a uniformly random bit string k of length n, i.e. $k \in \mathcal{K}$.
- Enc(k, m) : it outputs the ciphertext $c = k \oplus m$.
- Dec(k, c) : it recovers the message computing $m = k \oplus c$.

Used between the White House and the Kremlin during the Cold War.

Security of OTP

Theorem

The one time pad (OTP) encryption scheme is perfectly secret.

Security of OTP

Theorem

The one time pad (OTP) encryption scheme is perfectly secret.

Proof.

$$\begin{aligned}\Pr(C = c | M = m) &= \Pr(M \oplus K = c | M = m) \\ &= \Pr(m \oplus K = c) \\ &= \Pr(K = m \oplus c) = \frac{1}{2^n}\end{aligned}$$

since keys are chosen uniformly at random.

Security of OTP

Theorem

The one time pad (OTP) encryption scheme is perfectly secret.

Proof.

$$\begin{aligned}\Pr(C = c | M = m) &= \Pr(M \oplus K = c | M = m) \\ &= \Pr(m \oplus K = c) \\ &= \Pr(K = m \oplus c) = \frac{1}{2^n}\end{aligned}$$

since keys are chosen uniformly at random.
Therefore, for any m_0, m_1, we have

$$\Pr(C = c | M = m_0) = \frac{1}{2^n} = \Pr(C = c | M = m_1).$$

□

OTP is perfectly secret, but is it practical?

When a key k is used to encrypt more than one message, the ciphertexts leak information:

$$c_1 := m_1 \oplus k, c_2 := m_2 \oplus k \quad \Rightarrow \quad c_1 \oplus c_2 = m_1 \oplus m_2.$$

OTP is perfectly secret, but is it practical?

When a key k is used to encrypt more than one message, the ciphertexts leak information:

$$c_1 := m_1 \oplus k, c_2 := m_2 \oplus k \quad \Rightarrow \quad c_1 \oplus c_2 = m_1 \oplus m_2.$$

To securely exchange a message $m \in \{0,1\}^n$ we have to securely exchange $k \in \{0,1\}^n$, which can be used only once.

OTP is perfectly secret, but is it practical?

When a key k is used to encrypt more than one message, the ciphertexts leak information:

$$c_1 := m_1 \oplus k, c_2 := m_2 \oplus k \quad \Rightarrow \quad c_1 \oplus c_2 = m_1 \oplus m_2.$$

To securely exchange a message $m \in \{0,1\}^n$ we have to securely exchange $k \in \{0,1\}^n$, which can be used only once.

You might as well directly exchange m!

Is the impracticality of OTP an exception?

Theorem

If an encryption scheme is perfectly secret, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Is the impracticality of OTP an exception?

Theorem

If an encryption scheme is perfectly secret, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof.

We show that if $|\mathcal{K}| < |\mathcal{M}|$ we do not have perfect secrecy.

Is the impracticality of OTP an exception?

Theorem

If an encryption scheme is perfectly secret, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof.

We show that if $|\mathcal{K}| < |\mathcal{M}|$ we do not have perfect secrecy.

Let $\Pr_{\mathcal{M}}$ be the uniform distribution over $\mathcal{M}$. For $c \in \mathcal{C}$ define:

$$\mathcal{M}(c) := \{m \mid m = \mathrm{Dec}(k, c) \text{ for some } k \in \mathcal{K}\}$$

Since $|\mathcal{M}(c)| \leq |\mathcal{K}|$ and we are assuming $|\mathcal{K}| < |\mathcal{M}|$, there exists $m' \in \mathcal{M}$ s.t. $m' \notin \mathcal{M}(c)$. Therefore:

$$\Pr(M = m' | C = c) = 0 \neq \Pr(M = m') = \frac{1}{2^n}.$$

□

From Perfect to Computational Secrecy

- Perfect secrecy: no leakage of information about the plaintext even when $\mathcal{A}$ has unlimited computational power.

From Perfect to Computational Secrecy

- Perfect secrecy: no leakage of information about the plaintext even when $\mathcal{A}$ has unlimited computational power.

- Computational secrecy: an encryption scheme can be considered secure even if it leaks some information with a probability which is very small when $\mathcal{A}$ has limited power.

From Perfect to Computational Secrecy

- Perfect secrecy: no leakage of information about the plaintext even when $\mathcal{A}$ has unlimited computational power.
- Computational secrecy: an encryption scheme can be considered secure even if it leaks some information with a probability which is very small when $\mathcal{A}$ has limited power.

Real-world application: happy with a scheme that leaks information with probability at most 2^{-60} over 200 years using the fastest supercomputers!

Further Reading I

- Nadhem J AlFardan, Daniel J Bernstein, Kenneth G Paterson, Bertram Poettering, and Jacob CN Schuldt.
  On the security of RC4 in TLS.
  In 22nd USENIX Security Symposium (USENIX Security 13), pages 305–320, 2013.
- Boaz Barak and Shai Halevi.
  A model and architecture for pseudo-random generation with applications to/dev/random.
  In Proceedings of the 12th ACM conference on Computer and communications security, pages 203–212. ACM, 2005.
- Daniel J Bernstein.
  The Salsa20 Family of Stream Ciphers.
  In New stream cipher designs, pages 84–97. Springer, 2008.

Further Reading II

Lenore Blum, Manuel Blum, and Mike Shub.
A simple unpredictable pseudo-random number generator.
SIAM Journal on computing, 15(2):364–383, 1986.

Christian Cachin.
Entropy measures and unconditional security in cryptography.
PhD thesis, ETH Zurich, 1997.

Scott Fluhrer, Itsik Mantin, and Adi Shamir.
Weaknesses in the key scheduling algorithm of RC4.
In Selected areas in cryptography, pages 1–24. Springer, 2001.

Further Reading III

Christina Garman, Kenneth G Paterson, and Thyla Van der Merwe.
Attacks only get better: Password recovery attacks against RC4 in TLS.
In 24th USENIX Security Symposium (USENIX Security 15), pages 113–128, 2015.

Itsik Mantin and Adi Shamir.
A practical attack on broadcast RC4.
In Fast Software Encryption, pages 152–164. Springer, 2002.