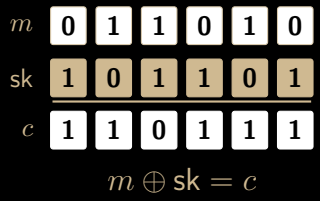
Lecture 01: The One-Time Pad

Correctness, privacy, and security



The puzzle: what can Eve rule out?

Eve intercepts only

$$c = 110111.$$

What does this reveal about the unknown message m?

Guiding question

Can two different messages produce the same ciphertext?

candidate m	matching sk	$m \oplus$ sk
000000	110111	110111
011010	101101	110111
111111	001000	110111

Every candidate message has a matching secret key.

Roadmap

By the end of the lecture, we will be able to

1. state the one-time pad precisely;
2. distinguish correctness, privacy, and security;
3. prove correctness by an XOR identity;
4. formalize privacy as "the ciphertext reveals no additional information";
5. prove privacy by a one-line bijection argument and conclude security;
6. analyze the zero key, group generalizations, and key reuse.

Course convention: correctness, privacy, security

Correctness

Decryption of an encrypted message returns the original message:

$$\mathsf{Dec}_{\mathsf{sk}}\big(\mathsf{Enc}_{\mathsf{sk}}(m)\big) = m.$$

Privacy

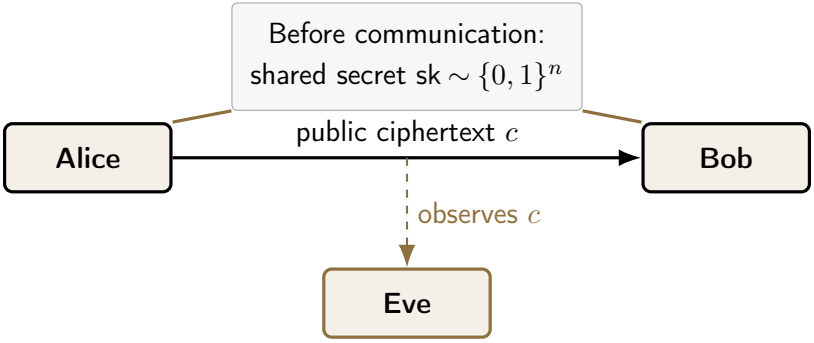
The ciphertext reveals no additional information about the message.

Security

An encryption scheme is secure when it is both correct and private:

$$\boxed{\text{security} = \text{correctness} + \text{privacy}.}$$

Communication model



Threat model

We hide the message content; we do not hide that communication occurred, its timing, or its length.

The one-time pad in three lines

1. Secret-key generation

$$\mathsf{sk} \sim \{0,1\}^n.$$

Alice and Bob share the same uniformly random secret key.

2. Encryption

$$c = \mathsf{Enc}_{\mathsf{sk}}(m) := m \oplus \mathsf{sk}.$$

Alice sends c over the public channel.

3. Decryption

$$m' = \mathsf{Dec}_{\mathsf{sk}}(c) := c \oplus \mathsf{sk}.$$

Bob uses the shared secret key to recover the message.

Assumptions that matter for privacy

The secret key is hidden, uniform over all of $\{0,1\}^n$ (including 0^n), as long as the message, and used for only one message.

Worked example

	1	2	3	4	5	6
m	0	1	1	0	1	0
sk	1	0	1	1	0	1
$c = m \oplus \mathsf{sk}$	1	1	0	1	1	1

$$011010 \oplus 101101 = 110111, \qquad 110111 \oplus 101101 = 011010.$$

The same operation goes both ways

XOR with the shared secret key encrypts; XOR with it again decrypts.

Correctness is an algebraic identity

For every $m, \mathsf{sk} \in \{0,1\}^n$,

$$\mathsf{Dec}_{\mathsf{sk}}\big(\mathsf{Enc}_{\mathsf{sk}}(m)\big) = m.$$

Indeed,

$$\begin{aligned}\mathsf{Dec}_{\mathsf{sk}}\big(\mathsf{Enc}_{\mathsf{sk}}(m)\big) &= (m \oplus \mathsf{sk}) \oplus \mathsf{sk} \\ &= m \oplus (\mathsf{sk} \oplus \mathsf{sk}) \\ &= m \oplus 0^n \\ &= m.\end{aligned}$$

Three XOR facts

Associativity; $\mathsf{sk} \oplus \mathsf{sk} = 0^n$; and $m \oplus 0^n = m$.

Why correctness and privacy are both necessary

Correct but not private

$$\mathsf{Enc}_{\mathsf{sk}}(m) = m, \qquad \mathsf{Dec}_{\mathsf{sk}}(c) = c.$$

- Correctness holds.
- The ciphertext reveals m completely.
- Privacy fails; therefore the scheme is not secure.

Private but not correct

$$\mathsf{Enc}_{\mathsf{sk}}(m) = 0^n.$$

- The ciphertext reveals nothing about m.
- Bob cannot recover every possible m.
- Correctness fails; therefore the scheme is not secure.

The nontrivial goal

Achieve correctness and privacy simultaneously; only then do we obtain security.

What does privacy mean?

A secret-key encryption scheme is private in this setting if, for every $m_0, m_1, c \in \{0,1\}^n$,

$$\Pr_{\mathsf{sk}\sim\{0,1\}^n}[\mathsf{Enc}_{\mathsf{sk}}(m_0) = c] = \Pr_{\mathsf{sk}\sim\{0,1\}^n}[\mathsf{Enc}_{\mathsf{sk}}(m_1) = c]\,.$$

Interpretation

The ciphertext distribution is identical for every message; equivalently, observing c gives no additional information about the message, for any prior on m.

Terminology in the literature

This information-theoretic privacy notion is often called *perfect secrecy*. It is stronger than saying that recovering m is merely computationally difficult.

The bijection behind privacy

Fix $m, c \in \{0,1\}^n$. Solving $m \oplus \mathsf{sk} = c$ gives

$$\mathsf{sk} = m \oplus c.$$

Unique-key principle

Every message–ciphertext pair (m, c) has exactly one compatible secret key.

For example, when $m = 10$, XOR by m permutes the secret-key space:

secret key sk	00	01	10	11
$c = m \oplus \mathsf{sk}$	10	11	00	01

A uniform sk gives the same ciphertext distribution for every message.

Privacy of the one-time pad

Privacy theorem

For $\mathsf{sk} \sim \{0,1\}^n$, the one-time pad is private [Sha49]; this property is usually called perfect secrecy [BS23, Thm. 2.2].

Proof. Fix $m, c \in \{0,1\}^n$. The unique-key principle gives

$$\begin{aligned} \Pr_{\mathsf{sk} \sim \{0,1\}^n}[\mathsf{Enc}_{\mathsf{sk}}(m) = c] &= \Pr_{\mathsf{sk} \sim \{0,1\}^n}[\mathsf{sk} = m \oplus c] \\ &= 2^{-n}. \end{aligned}$$

This value is independent of m; hence every message induces exactly the same ciphertext distribution. □

Security conclusion

The one-time pad is correct and private; therefore, under our convention, it is secure.

Does $\mathsf{sk} = 0^n$ threaten privacy?

A zero-key execution

$$\mathsf{sk} = 0^n \quad \Longrightarrow \quad c = m, \quad \Pr[\mathsf{sk} = 0^n] = 2^{-n}.$$

The bits on the wire equal the message. But Eve sees c, not the sampled secret key. Given c, every candidate $\widetilde{m}$ has one compatible key:

$$\widetilde{\mathsf{sk}} = \widetilde{m} \oplus c.$$

Thus $\widetilde{m} = c$ is not recognizable as the true message; it merely corresponds to $\widetilde{\mathsf{sk}} = 0^n$.

With the full key space

For every $m, c \in \{0,1\}^n$,

$$\Pr_{\mathsf{sk} \sim \{0,1\}^n}[\mathsf{Enc}_{\mathsf{sk}}(m) = c] = 2^{-n}.$$

The ciphertext distribution is independent of m: privacy holds.

Should we forbid 0^n?

For $\mathsf{sk} \sim \{0,1\}^n \setminus \{0^n\}$,

$$\Pr[\mathsf{Enc}_{\mathsf{sk}}(m) = c] = \begin{cases} 0, & c = m, \\ \dfrac{1}{2^n - 1}, & c \neq m. \end{cases}$$

Now the distribution depends on m: observing c rules out the candidate message $m = c$. Hence privacy fails.

Answer

Keep 0^n. Removing it preserves correctness but breaks privacy; therefore the modified scheme is not secure. Privacy also requires sk to remain hidden: revealing any key value permits immediate decryption.

The one-time pad is a group construction

Let G be any finite group with operation $\star$. Choose $\mathsf{sk} \sim G$ uniformly, and define

$$c = \mathsf{Enc}_{\mathsf{sk}}(m) := m \star \mathsf{sk}, \qquad m = \mathsf{Dec}_{\mathsf{sk}}(c) := c \star \mathsf{sk}^{-1}.$$

Why correctness and privacy extend

$$(m \star \mathsf{sk}) \star \mathsf{sk}^{-1} = m,$$

$$m \star \mathsf{sk} = c \iff \mathsf{sk} = m^{-1} \star c.$$

The first identity proves correctness. The bijection $\mathsf{sk} \mapsto m \star \mathsf{sk}$ makes the ciphertext uniform for every m, proving privacy. Hence the group-based scheme is secure.

Crypto-relevant examples

$(\mathbb{Z}/2\mathbb{Z})^n$	XOR
$(\mathbb{Z}/N\mathbb{Z}, +)$	addition modulo N
$(\mathbb{F}_q, +),\ \mathbb{F}_q^\times$	field addition/multiplication
$E(\mathbb{F}_q)$	elliptic-curve point addition

See [BS23, Chs. 10 and 15].

We will briefly cover these group structures in the upcoming lectures.

Why is it called a *one-time* pad?

Suppose the same secret key sk encrypts two messages:

$$c_1 = m_1 \oplus \mathsf{sk}, \qquad c_2 = m_2 \oplus \mathsf{sk}.$$

Then Eve can compute

$$\begin{aligned} c_1 \oplus c_2 &= (m_1 \oplus \mathsf{sk}) \oplus (m_2 \oplus \mathsf{sk}) \\ &= m_1 \oplus m_2. \end{aligned}$$

Why privacy fails

The secret key cancels, exposing a deterministic relation between the two plaintexts. Natural-language redundancy or partial knowledge can then reveal substantial information [BS23, Sec. 3.3.1]. Correctness still holds, but privacy fails; therefore key reuse is not secure.

Takeaways

1. **Construction:** $c = m \oplus \mathsf{sk}$ and $m = c \oplus \mathsf{sk}$.
2. **Correctness:** decryption of the encrypted message returns the original message.
3. **Privacy:** the ciphertext reveals no additional information about the message.
4. **Security:** the one-time pad is secure because it is both correct and private.
5. **Group viewpoint:** XOR may be replaced by the operation of any finite group.
6. **Essential assumptions:** sk is uniform over all of $\{0,1\}^n$ (including 0^n), hidden, message-length, and never reused.

The central privacy proof pattern

Look for a measure-preserving bijection that makes the ciphertext distribution independent of the message.

References

[BS23] Dan Boneh and Victor Shoup.

A Graduate Course in Applied Cryptography, 2023.

Version 0.6, January 2023.

URL: https://toc.cryptobook.us/book.pdf.

[KL20] Jonathan Katz and Yehuda Lindell.

Introduction to Modern Cryptography.

CRC Press, 3 edition, 2020.

[Sha49] Claude E. Shannon.

Communication theory of secrecy systems.

Bell System Technical Journal, 28(4):656–715, 1949.

doi:10.1002/j.1538-7305.1949.tb00928.x.