Part I

Information-Theoretic Security Model

1. Information-Theoretic Security Model

Assumptions

- We are looking for a definition that captures our confidentiality needs in presence of passive attackers. No message integrity or authentication.
- We have access to an unlimited supply of independent, unbiased random bits
  1. Collect high-entropy data (= from physical source)
  2. Remove correlation and bias (*whitening*)
- The message probability distribution is public.
- The message and the key are independent.

Shift Cipher

Oldest encryption scheme (Caesar). Messages are strings of any size of uppercase letters from the alphabet $\{\mathtt{A},\ldots,\mathtt{Z}\}^*$.[1] Let's encode $\mathtt{A}=0,\ldots,\mathtt{Z}=25$.

Definition (Shift Cipher)

Message space is $\mathcal{M}=\mathbb{Z}_{26}^*$. Key space is $\mathcal{K}=\mathcal{M}$.
Let $m\in\mathcal{M}$ be a message of size l, then $m_1,m_2,\ldots,m_l$ are the letters of the message.

Gen k uniformly at random from $\mathbb{Z}_{26}$

Enc $c_i = m_i + k \bmod 26$

Dec $m_i = c_i - k \bmod 26$

[1] Between braces we write the alphabet. Superscript indicates message size (* = any).

Example 1

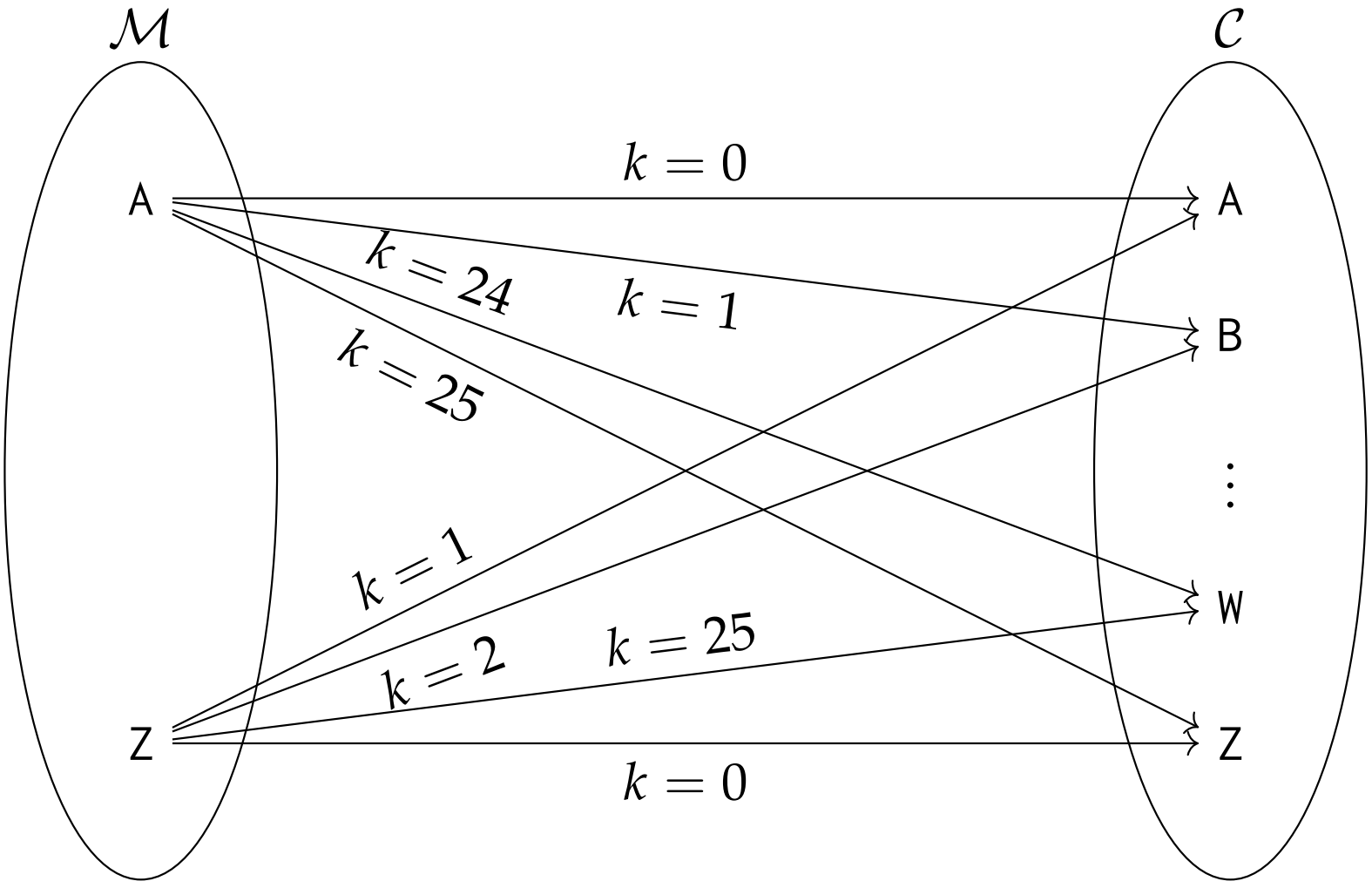
Problem Statement

Assume that $\mathcal{M} = \{\mathtt{A}, \mathtt{Z}\}$. Alice chooses $m = \mathtt{A}$ with probability 0.7 and $m = \mathtt{Z}$ with probability 0.3. Alice encrypts the message with some random key.
Eve, an eavesdropper, sees $c = \mathtt{B}$. What can she say about the plaintext?

Formally, *a priori* probability is $\Pr[m = \mathtt{A}] = 0.7$, $\Pr[m = \mathtt{Z}] = 0.3$. What is $\Pr[m = \mathtt{A} | c = \mathtt{B}]$?

Example 1

Representation



Example 1

Given a plaintext m and a ciphertext c, there is one and only one key that maps m into c.
In our case $c = \mathsf{B}$ if and only if either:

1. $m = \mathsf{A}$ and $k = 1$
2. or $m = \mathsf{Z}$ and $k = 2$

So,

$$\Pr[c = \mathsf{B} | m = \mathsf{A}] = \Pr[k = 1] = 1/26$$
$$\Pr[c = \mathsf{B} | m = \mathsf{Z}] = \Pr[k = 2] = 1/26$$

Thus, the *a priori* probability of seeing ciphertext $c = \mathsf{B}$ is:

$$\Pr[c = \mathsf{B}] = \Pr[c = \mathsf{B} | m = \mathsf{A}] \Pr[m = \mathsf{A}] +$$
$$\Pr[c = \mathsf{B} | m = \mathsf{Z}] \Pr[m = \mathsf{Z}] = 1/26(0.7 + 0.3) = 1/26$$

Example 1

Using Bayes' Theorem we have:

$$\Pr[m = \mathsf{A}|c = \mathsf{B}] = \frac{\Pr[c = \mathsf{B}|m = \mathsf{A}]\Pr[m = \mathsf{A}]}{\Pr[c = \mathsf{B}]} = \frac{1/26 \times \Pr[m = \mathsf{A}]}{1/26} = \Pr[m = \mathsf{A}] = 0.7$$

The same holds for $m = \mathsf{Z}$.
So, knowledge of the ciphertext does not change the attacker's knowledge of the probabilities of the messages. The attacker learns nothing.

Information Entropy

Definition

Given a message m taken from a set of messages $\{m_1, \ldots, m_N\}$ with probabilities $p(m_i)$ $1 \leq i \leq N$, the source entropy is

$$H(m) = -\sum_{i=1}^{N} p_i \log_2 p_i$$

Information entropy measures the minimum number of bits necessary to encode the source messages.

Given a message m taken from a set of messages $\{m_i\}$ with probabilities $p(m_i)$ and a message c taken from a set of messages $\{c_j\}$ with probabilities $p(c_j)$ and joint probabilities $p(m_i, c_j)$, the joint entropy is

$$H(m, c) = -\sum_{i,j} p(m_i, c_j) \log 2p(m_i, c_j)$$

Conditional Entropy

Given a message m taken from a set of messages $\{m_i\}$ with probabilities $p(m_i)$ and a message c taken from a set of messages $\{c_j\}$ with probabilities $p(c_j)$ and joint probabilities $p(m_i, c_j)$, the conditional entropy is

$$H(c|m) = \sum_i H(c|m_i) \Pr[m_i]$$

Chain Rule

$$H(m,c) = H(m) + H(c|m) = H(c) + H(m|c)$$

Information Entropy

Properties

Bayes' Theorem

$$H(m|c) = H(c|m) - H(c) + H(m)$$

Mutual Information

$$I(m;c) = H(m) - H(m|c) = H(c) - H(c|m)$$

Mutual information is equal to zero if and only if the two messages are independent.

Example 1

Analogous calculations can be done using information entropy. The entropy of the message source is:

$$H(m) = -\Pr[m = \mathsf{A}] \log_2 \Pr[m = \mathsf{A}] - \Pr[m = \mathsf{Z}] \log_2 \Pr[m = \mathsf{Z}] = 0.88\,\text{bit}$$

Given a plaintext, all ciphertexts are equally likely, so

$$H(c|m) = 26 \times \frac{1}{26} \log_2 26 = 4.7\,\text{bit}$$

Example 1

We already know that

$$\Pr[c = \mathsf{A}] = \cdots = \Pr[c = \mathsf{Z}] = 1/26$$

thus $H(c) = 4.7\,\text{bit}$.
Therefore:

$$I(m;c) = H(c) - H(c|m) = 0$$

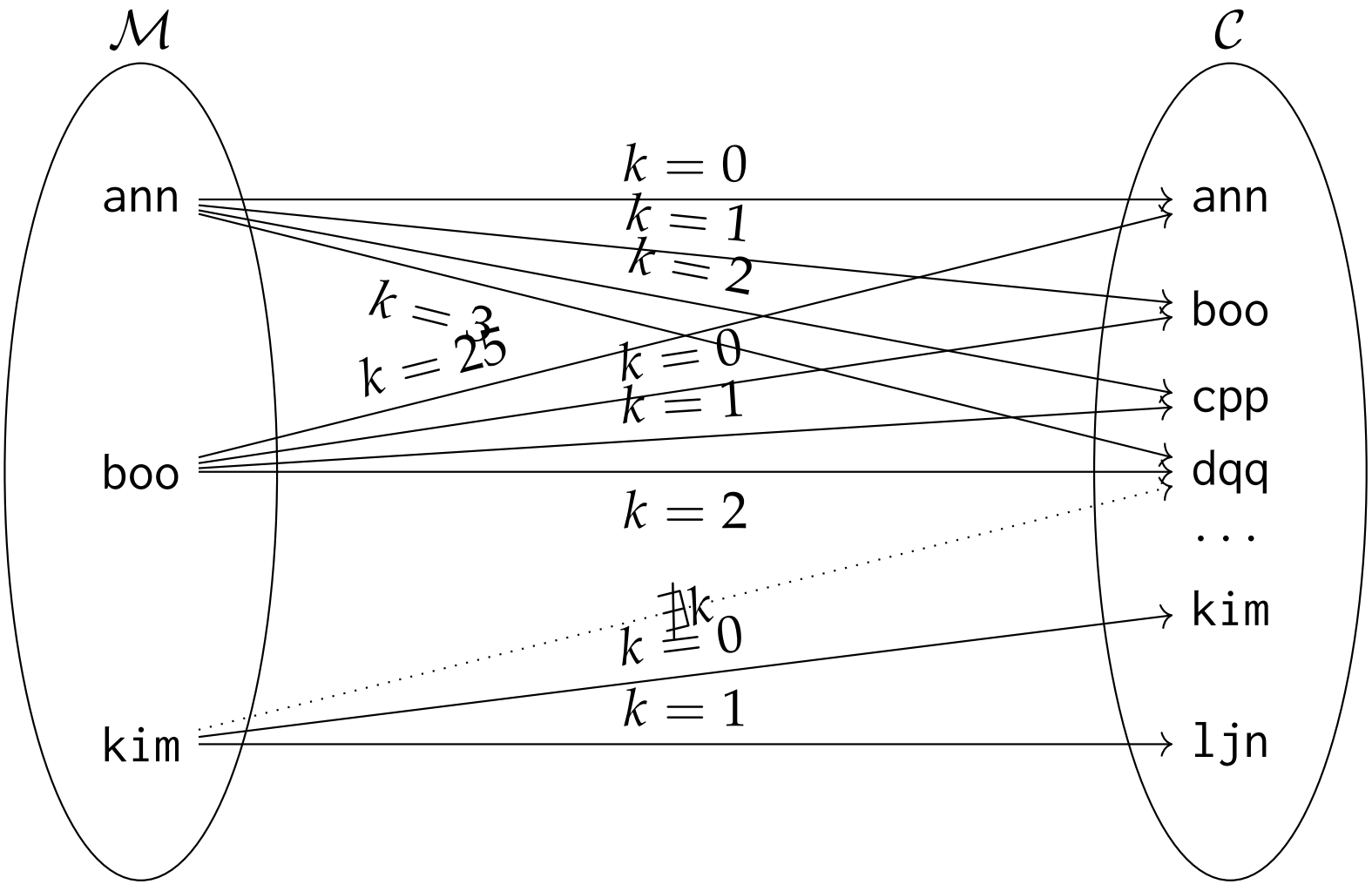
No information is learned.

Example 2

Assume that $\Pr[m = \texttt{kim}] = 0.5$, $\Pr[m = \texttt{ann}] = 0.2$, and $\Pr[m = \texttt{boo}] = 0.3$.

What is $\Pr[m = \texttt{ann} | c = \texttt{dqq}]$?

Representation



Example 2

This ciphertext occurs when $m = \mathsf{ann}$ and $k = 3$ or $m = \mathsf{boo}$ and $k = 2$. It cannot occur when $m = \mathtt{kim}$.
Thus, $\Pr[m = \mathsf{ann} | c = \mathsf{dqq}] = 0.4$, which is larger than the a priori probability 0.2.

Example 2

Analogous calculations can be done using information entropy. The entropy of the message source is:

$$H(m) = 1.49\,\text{bit}$$

Ciphertexts are not equally likely. There are only $26 + 26 = 52$ different CTs, half of which obtained from `kim` and half from ann and boo.

$$H(c) = -52\frac{1}{52}\log_2\frac{1}{52} = 5.7\,\text{bit}$$

Given a plaintex, all ciphertexts are equally likely:
$H(c|m) = 4.7\,\text{bit}$.

Example 2

$$I(m;c) = H(c) - H(c|m) = 1\,\text{bit}$$

meaning that knowledge of c gives us 1 bit of information.
This does not tell us what is the algorithm to obtain this bit.
Neither whether this algorithm is efficient. It only tells us that this algorithm exists.
In practice, we see the following algorithm gives 1 bit of information.

if last two letters of cipheterxt are the same **then**
    plaintext is not `kim`
else
    plaintext is `kim`
end if

1. Information-Theoretic Security Model

The One Time Pad (OTP)

Due to Vernam (1917). Here discussed with a binary alphabet:

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

Definition (One Time Pad (OTP))

Gen k is a random string of n bits

Enc $c_i = k_i \oplus m_i$ (bit-to-bit XOR)

Dec $m_i = k_i \oplus c_i$ (bit-to-bit XOR)

Very simple. The key is as long as the message.

The One Time Pad (OTP)

Correctness

Basic proof of correctness:

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = m$$

Is OTP Secure?

We need the description of an attack scenario:

- A description of the attacker's capabilities.
- A precise definition of security.

At first we will assume a Ciphertext-only attack: the attacker knows a fragment of ciphertext and nothing else.

Wrong Definition of Security

First Attempt

First attempt: *the attacker cannot recover the key*.
This definition is not satisfactory. With this definition a cipher of the kind:

$$\mathrm{Enc}(k, m) = m$$

would be secure, which is clearly not what we want.

Wrong Definition of Security

Second Attempt

Second attempt: *the attacker cannot recover the plaintext*.
This definition is not satisfactory. With this definition the ciphertext would be "secure" even if the attacker can recover most of the plaintext. For example a cipher of the kind:

$$\mathsf{Enc}(k, m_1 \| m_2) = m_1 \| (k \oplus m_2)$$

would be secure.

1. Information-Theoretic Security Model

Perfect Secrecy

Shannon (1949) attempt: *the attacker obtains no information about the plaintext*.

Definition (Perfect Secrecy)

A cipher $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has *perfect secrecy* if for any pair of messages (m_0, m_1), for any ciphertext c and for a key chosen uniformly at random, then

$$\Pr[\mathsf{Enc}(k, m_0) = c] = \Pr[\mathsf{Enc}(k, m_1) = c]$$

Perfect Secrecy

- Given the CT c, the attacker cannot tell if the PT is m_0 or m_1, for all m_0, m_1, for all c, for all k
- An attacker with unbounded computational power learns nothing about PT (Information-Theoretic Security)
- CT-only attack is impossible, but we say nothing about other attacks

OTP has Perfect Secrecy

Theorem

OTP has perfect secrecy

Theorem

If a cipher has perfect secrecy, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Perfect secrecy implies that the key space must be at least as large as the message space. Note that:

- the condition is necessary, not sufficient
- OTP is the most efficient cipher with perfect secrecy, having $|\mathcal{K}| = |\mathcal{M}|$

Shannon's Theorem

Gives necessary and sufficient conditions for perfect secrecy.

Theorem (Shannon's Theorem)

A cipher $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with* $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C})|$ *has perfect secrecy if and only if:*

1. Gen *chooses keys uniformly at random.*
2. *for every* m, c, *there exists a unique key* k *such that* $\mathsf{Enc}(k, m) = c$.

Adversarial Indistingushability

We give an alternative formulation of the definition of perfect secrecy. (Will be useful later)
We have a Challenger, $\mathcal{C}$, who executes the encryption scheme honestly. She receives a single bit b as input.
A dishonest Adversary, $\mathcal{A}$, tries to guess the input bit b. It can be any algorithm and can do whatever is allowed by the security assumptions.
Our goal will be to prove that there exists no $\mathcal{A}$ capable of giving a guess b' better than giving random guesses.
We call any execution of $\mathcal{A}$ an experiment.

Adversarial Indistingushability

Consider the following experiment $b' = \mathsf{Exp}(b)$.

Experiment (Adversarial Indistingushability)

1. *$\mathcal{A}$ chooses and outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*
2. *$\mathcal{C}$ generates a key k using* Gen*, receives a random bit b as input, computes $c = \mathsf{Enc}(k, m_b)$, and sends c to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs a bit b'.*

The experiment succeeds if $b = b'$.

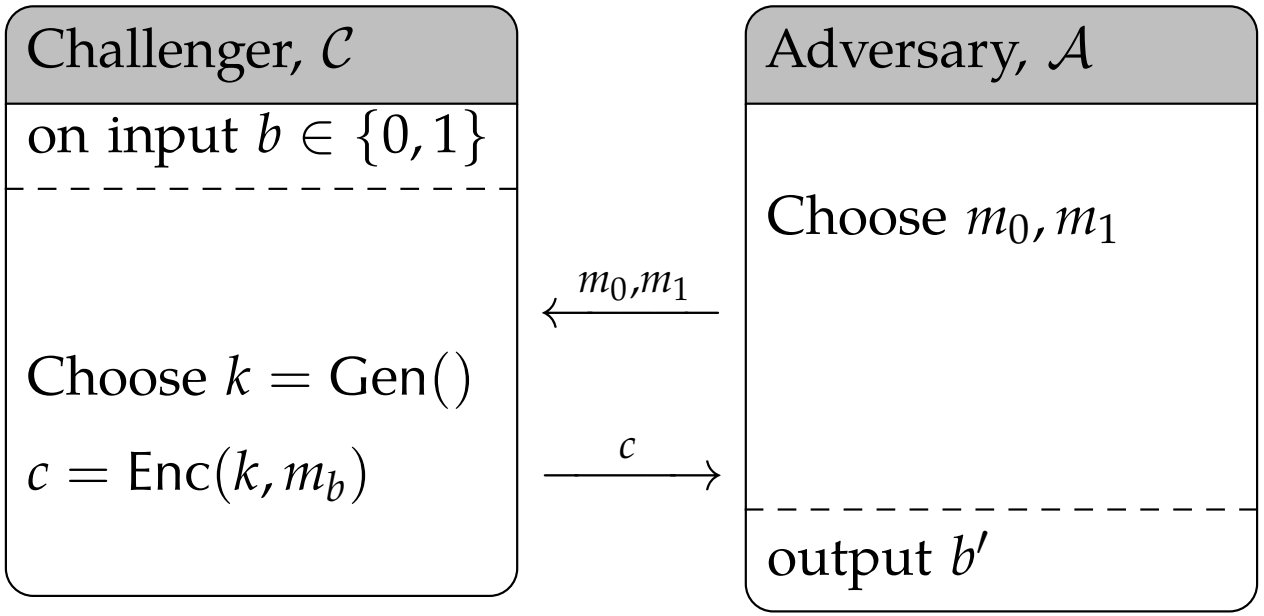
The Advantage of algorithm $\mathcal{A}$ is:

$$\mathrm{Adv}[\mathcal{A}] = |\Pr[\mathsf{Exp}(0) = 1] - \Pr[\mathsf{Exp}(1) = 1]|$$

It is trivial to find $\mathcal{A}$ that yields $\mathrm{Adv}[\mathcal{A}] = 0$. A cipher is perfectly secret if and only if it is impossible for any $\mathcal{A}$ to do better.

Adversarial Indistingushability

We will use also this graphical notation:



1. Information-Theoretic Security Model

Two-time pad

Suppose you use the same key twice. This attack violates the assumption that a new key is generated for each message.

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$

Then, $c_1 \oplus c_2 = m_1 \oplus m_2$.
Given $m_1 \oplus m_2$ the adversary can guess m_1, m_2 exploiting language redundancy.

Example

Server-to-client and client-to-server must use different keys.

Malleability

Modifications to the ciphertext have predictable impact on plaintext. This attack violates the assumption that the attacker is passive.

$$m \xrightarrow{\text{Enc}} k \oplus m \xrightarrow[\textit{Adversary}]{\oplus p} G(k) \oplus m \oplus p \xrightarrow{\text{Dec}} m \oplus p$$

Example

$$\text{Bob} = 0x42\,6F\,62 \qquad \text{Eve} = 0x45\,76\,65$$

$$p = \text{Bob} \oplus \text{Eve} = 0x07\,19\,07$$

$$\texttt{From: Bob} \xrightarrow{\text{Enc}} c \xrightarrow[\textit{Adversary}]{\oplus p} c \oplus p \xrightarrow{\text{Dec}} \texttt{From: Eve}$$