The One-Time Pad (OTP)

\[ M = C = K = \{0, 1\} \]

- **Encryption:**
  \[ \forall k \in K, \forall m \in M, E(k, m) = k \oplus m \]

\[ k = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, m = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, c = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \]

- **Decryption:**
  \[ \forall k \in K, \forall c \in C, D(k, c) = k \oplus c \]

\[ k = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, c = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, m = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \]

- **Consistency:**
  \[ D(k, E(k, m)) = k \oplus (k \oplus m) = m \]
The One-Time Pad (OTP)

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$
The One-Time Pad (OTP)

- \( \mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n \)
- Encryption: \( \forall k \in \mathcal{K}. \forall m \in \mathcal{M}. E(k, m) = k \oplus m \)
The One-Time Pad (OTP)

- \( \mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n \)
- Encryption: \( \forall k \in \mathcal{K}. \forall m \in \mathcal{M}. \, E(k, m) = k \oplus m \)

| \( k \) | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| \( m \) | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |

| \( c \) | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
The One-Time Pad (OTP)

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$
- Encryption: $\forall k \in \mathcal{K}. \forall m \in \mathcal{M}. E(k, m) = k \oplus m$

\[
\begin{align*}
k & = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \\
m & = 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \\
c & = 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0
\end{align*}
\]

- Decryption: $\forall k \in \mathcal{K}. \forall c \in \mathcal{C}. D(k, c) = k \oplus c$

\[
\begin{align*}
k & = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \\
c & = 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0
\end{align*}
\]
The One-Time Pad (OTP)

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$
- Encryption: $\forall k \in \mathcal{K}. \forall m \in \mathcal{M}. E(k, m) = k \oplus m$

\[
\begin{align*}
  k &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \\
  m &= 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \\
  c &= 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \\
\end{align*}
\]

- Decryption: $\forall k \in \mathcal{K}. \forall c \in \mathcal{C}. D(k, c) = k \oplus c$

\[
\begin{align*}
  k &= 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \\
  c &= 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \\
  m &= 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \\
\end{align*}
\]
The One-Time Pad (OTP)

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$
- Encryption: $\forall k \in \mathcal{K}. \forall m \in \mathcal{M}. E(k, m) = k \oplus m$


\[
\begin{array}{cccccccc}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}
\]

- Decryption: $\forall k \in \mathcal{K}. \forall c \in \mathcal{C}. D(k, c) = k \oplus c$


\[
\begin{array}{cccccccc}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}
\]

- Consistency: $D(k, E(k, m)) = k \oplus (k \oplus m) = m$
Perfect secrecy

Definition
A cipher \((E, D)\) over \((\mathcal{M}, \mathcal{C}, \mathcal{K})\) satisfies perfect secrecy if for all messages \(m_1, m_2 \in \mathcal{M}\) of same length \(|m_1| = |m_2|\), and for all ciphertexts \(c \in \mathcal{C}\)

\[
|Pr(E(k, m_1) = c) - Pr(E(k, m_2) = c)| \leq \epsilon
\]

where \(k \leftarrow \mathcal{K}\) and \(\epsilon\) is some “negligible quantity”.
Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof:
We first note that for all messages \( m \in M \) and all ciphertexts \( c \in C \):

\[
\Pr( E(k, m) = c) = \# \{ k \in K : k \oplus m = c \} = \# K = 1 \# K
\]

where \( k \leftarrow K \).

Thus, for all messages \( m_1, m_2 \in M \) and for all ciphertexts \( c \in C \):

\[
| \Pr( E(k, m_1) = c) - \Pr( E(k, m_2) = c) | \leq \frac{1}{\# K} \leq 0
\]
OTP satisfies perfect secrecy

Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages $m \in M$ and all ciphertexts $c \in C$

$$Pr(E(k, m) = c)$$

where $k \leftarrow K$. 
Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages $m \in \mathcal{M}$ and all ciphertexts $c \in \mathcal{C}$

$$Pr(E(k, m) = c) = \frac{\#\{k \in \mathcal{K}: k \oplus m = c\}}{\#\mathcal{K}}$$

where $k \leftarrow \mathcal{K}$. 
Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages \( m \in \mathcal{M} \) and all ciphertexts \( c \in \mathcal{C} \)

\[
Pr(E(k, m) = c) = \frac{\#\{k \in \mathcal{K}: k \oplus m = c\}}{\#\mathcal{K}}
\]
\[
= \frac{\#\{k \in \mathcal{K}: k = m \oplus c\}}{\#\mathcal{K}}
\]

where \( k \leftarrow_{r} \mathcal{K} \).
OTP satisfies perfect secrecy

Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages \( m \in \mathcal{M} \) and all ciphertexts \( c \in \mathcal{C} \)

\[
Pr(E(k, m) = c) = \frac{\#\{k \in \mathcal{K}: k \oplus m = c\}}{\#\mathcal{K}}
\]

\[
= \frac{\#\{k \in \mathcal{K}: k = m \oplus c\}}{\#\mathcal{K}}
\]

\[
= \frac{1}{\#\mathcal{K}}
\]

where \( k \leftarrow \mathcal{K} \).
Theorem (Shannon 1949)

The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages \( m \in M \) and all ciphertexts \( c \in C \)

\[
Pr(E(k, m) = c) = \frac{\#\{k \in K: k \oplus m = c\}}{\#K}
\]

\[
= \frac{\#\{k \in K: k = m \oplus c\}}{\#K}
\]

\[
= \frac{1}{\#K}
\]

where \( k \leftarrow^\$ K \).

Thus, for all messages \( m_1, m_2 \in M \), and for all ciphertexts \( c \in C \)

\[
|Pr(E(k, m_1) = c) - Pr(E(k, m_2) = c)| \leq \varepsilon
\]
The One-Time Pad satisfies perfect secrecy

Proof: We first note that for all messages $m \in \mathcal{M}$ and all ciphertexts $c \in \mathcal{C}$

$$
Pr(E(k, m) = c) = \frac{\#\{k \in \mathcal{K} : k \oplus m = c\}}{\#\mathcal{K}}
$$

$$
= \frac{\#\{k \in \mathcal{K} : k = m \oplus c\}}{\#\mathcal{K}}
$$

$$
= \frac{1}{\#\mathcal{K}}
$$

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

Thus, for all messages $m_1, m_2 \in \mathcal{M}$, and for all ciphertexts $c \in \mathcal{C}$

$$
|Pr(E(k, m_1) = c) - Pr(E(k, m_2) = c)| \leq \left| \frac{1}{\#\mathcal{K}} - \frac{1}{\#\mathcal{K}} \right| = 0
$$
Limitations of OTP

- **Key-length**: The key should be as long as the plaintext.
- **Getting true randomness**: The key should not be guessable from an attacker.
- **Perfect secrecy does not capture all possible attacks**: OTP is subject to two-time pad attacks given $m_1 \oplus k$ and $m_2 \oplus k$, we can compute $m_1 \oplus m_2 = (m_1 \oplus k) \oplus (m_2 \oplus k)$.
- **English has enough redundancy s.t.** $m_1 \oplus m_2 \rightarrow m_1, m_2$
- **OTP is malleable**: given the ciphertext $c = E(k, m)$ with $m$ to bob: $m_0$, it is possible to compute the ciphertext $c' = E(k, m'_0)$ with $m'_0$ to eve: $m_0 \oplus c' \oplus "00...00" \oplus "00...00"$.
Limitations of OTP

- Key-length!
  - The key should be as long as the plaintext.

\[
\begin{align*}
\text{English has enough redundancy s.t.} & \quad m_1 \oplus m_2 \rightarrow m_1, m_2
\end{align*}
\]

OTP is malleable given the ciphertext \( c = E(k, m) \) with \( m = \text{to bob} \):

- It is possible to compute the ciphertext \( c' = E(k, m') \) with \( m' = \text{to eve} \):

\[
\begin{align*}
E(k, m) \oplus \text{"to bob": 00...00"} \oplus \text{"to eve": 00...00"}
\end{align*}
\]
Limitations of OTP

- Key-length!
  - The key should be as long as the plaintext.

- Getting true randomness!
  - The key should not be guessable from an attacker.
Limitations of OTP

▶ Key-length!
  ▶ The key should be as long as the plaintext.

▶ Getting true randomness!
  ▶ The key should not be guessable from an attacker.

▶ Perfect secrecy does not capture all possible attacks
Limitations of OTP

- Key-length!
  - The key should be as long as the plaintext.

- Getting true randomness!
  - The key should not be guessable from an attacker.

- Perfect secrecy does not capture all possible attacks
  - OTP is subject to two-time pad attacks
    given $m_1 \oplus k$ and $m_2 \oplus k$, we can compute
    $m_1 \oplus m_2 = (m_1 \oplus k) \oplus (m_2 \oplus k)$
    English has enough redundancy s.t. $m_1 \oplus m_2 \rightarrow m_1, m_2$
Limitations of OTP

- Key-length!
  - The key should be as long as the plaintext.

- Getting true randomness!
  - The key should not be guessable from an attacker.

- Perfect secrecy does not capture all possible attacks
  - OTP is subject to two-time pad attacks
    given $m_1 \oplus k$ and $m_2 \oplus k$, we can compute
    $m_1 \oplus m_2 = (m_1 \oplus k) \oplus (m_2 \oplus k)$
    English has enough redundancy s.t. $m_1 \oplus m_2 \rightarrow m_1, m_2$

  - OTP is malleable
    given the ciphertext $c = E(k, m)$ with $m = \text{to bob} : m_0$, it is possible to compute the ciphertext $c' = E(k, m')$ with $m' = \text{to eve} : m_0$
    $c' := c \oplus "\text{to bob}: 00\ldots00" \oplus "\text{to eve}: 00\ldots00"$
Stream ciphers

- Goal: make the OTP practical
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random

Encryption using a PRG $G$:
$$E(k, m) = G(k) \oplus m$$

Decryption using a PRG $G$:
$$D(k, c) = G(k) \oplus c$$

Stream ciphers are subject to two-time pad attacks
Stream ciphers are malleable
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random
  - The key will be generated from a key seed using a Pseudo-Random Generator (PRG)
    \[ G : \{0, 1\}^s \rightarrow \{0, 1\}^n \text{ with } s << n \]

- Stream ciphers are subject to two-time pad attacks
- Stream ciphers are malleable
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random
  - The key will be generated from a key seed using a Pseudo-Random Generator (PRG)
    \[ G : \{0, 1\}^s \rightarrow \{0, 1\}^n \text{ with } s << n \]
- Encryption using a PRG \( G \): \( E(k, m) = G(k) \oplus m \)
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random
  - The key will be generated from a key seed using a Pseudo-Random Generator (PRG)
    \[ G : \{0, 1\}^s \rightarrow \{0, 1\}^n \text{ with } s << n \]
- Encryption using a PRG \( G \):
  \[ E(k, m) = G(k) \oplus m \]
- Decryption using a PRG \( G \):
  \[ D(k, c) = G(k) \oplus c \]
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random
  - The key will be generated from a key seed using a Pseudo-Random Generator (PRG)
    \[ G : \{0, 1\}^s \to \{0, 1\}^n \text{ with } s << n \]
- Encryption using a PRG \( G \): \( E(k, m) = G(k) \oplus m \)
- Decryption using a PRG \( G \): \( D(k, c) = G(k) \oplus c \)
- Stream ciphers are subject to two-time pad attacks
Stream ciphers

- Goal: make the OTP practical
- Idea: use a pseudorandom key rather than a really random key
  - The key will not really be random, but will look random
  - The key will be generated from a key seed using a Pseudo-Random Generator (PRG)
    \[ G : \{0, 1\}^s \rightarrow \{0, 1\}^n \text{ with } s << n \]
- Encryption using a PRG \( G \): \( E(k, m) = G(k) \oplus m \)
- Decryption using a PRG \( G \): \( D(k, c) = G(k) \oplus c \)
- Stream ciphers are subject to two-time pad attacks
- Stream ciphers are malleable
RC4

- Stream cipher invented by Ron Rivest in 1987

- Consists of 2 phases:
  - Initialisation
  - Keystream generation

- Seed: 2048 bits

- Main data structure: array $S$ of 256 bytes.

- Used in HTTPS and WEP

- Weaknesses of RC4:
  - First bytes are biased → drop the first 256 generated bytes
  - Subject to related keys attacks → choose randomly generated keys as seeds
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

- **Seed** $k$:
  - 2048 bits

- **Keystream generation**:
  - 1 byte per round

Main data structure: array $S$ of 256 bytes.

Used in HTTPS and WEP.

Weaknesses of RC4:
- First bytes are biased → drop the first 256 generated bytes
- Subject to related keys attacks → choose randomly generated keys as seeds
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

- **Initialization**
- **Keystream generation**

Main data structure: array $S$ of 256 bytes.

Weaknesses of RC4:
- First bytes are biased → drop the first to 256 generated bytes
- Subject to related keys attacks → choose randomly generated keys as seeds
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

- **Seed** $k$ of 2048 bits
- **Keystream generation**

Main data structure: array $S$ of 256 bytes.

Used in HTTPS and WEP.
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

Main data structure: array $S$ of 256 bytes.

Used in HTTPS and WEP

Weaknesses of RC4:
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

- **initialisation**
- **keystream generation**

Main data structure: array $S$ of 256 bytes.

Used in HTTPS and WEP

Weaknesses of RC4:

- first bytes are biased
  → drop the first to 256 generated bytes
Stream cipher invented by Ron Rivest in 1987

Consists of 2 phases:

Main data structure: array $S$ of 256 bytes.

Used in HTTPS and WEP

Weaknesses of RC4:

- first bytes are biased
  - drop the first to 256 generated bytes
- subject to related keys attacks
  - choose randomly generated keys as seeds
for $i := 0$ to 255 do
    $S[i] := i$
end

$j := 0$

for $i := 0$ to 255 do
    $j := (j + S[i] + K[i \mod |K|]) \mod 256$
    swap($S[i], S[j]$)
end

$i := 0$

$j := 0$
RC4: key stream generation

while generatingOutput
  \[ i := i + 1 \pmod{256} \]
  \[ j := j + S[i] \pmod{256} \]
  \[ \text{swap}(S[i], S[j]) \]
  \[ \text{output}(S[S[i] + S[j] \pmod{256}]) \]
end
WEP uses RC4

Initialisation Vector (IV): 24-bits long string
Weaknesses of WEP

- Two-time pad attack: IV is 24 bits long, so the key is reused after at most $2^{24}$ frames. Use longer IVs.

- Fluhrer, Mantin and Shamir (FMS) attack (related keys attack):
  - The keys only differ in the 24 bits IV.
  - First bytes of key stream known because standard headers are always sent.
  - For certain IVs, knowing $m$ bytes of key and keystream means you can deduce byte $m + 1$ of the key.

Remark: The FMS attack does not apply to RC4-based SSL (TLS), since SSL generates the encryption keys it uses for RC4 by hashing, meaning that different SSL sessions have unrelated keys.
Weaknesses of WEP

- two-time pad attack: IV is 24 bits long, so the key is reused after at most $2^{24}$ frames
  → use longer IVs

Remark
The FMS attack does not apply to RC4-based SSL (TLS), since SSL generates the encryption keys it uses for RC4 by hashing, meaning that different SSL sessions have unrelated keys.
Weaknesses of WEP

- two-time pad attack: IV is 24 bits long, so the key is reused after at most $2^{24}$ frames
  \[\rightarrow\] use longer IVs

- Fluhrer, Mantin and Shamir (FMS) attack (related keys attack):
  - the keys only differ in the 24 bits IV
  - first bytes of key stream known because standard headers are always sent
  - for certain IVs knowing $m$ bytes of key and keystream means you can deduce byte $m + 1$ of key
  \[\rightarrow\] instead of using related IVs, generate IVs using a PRG

Remark: The FMS attack does not apply to RC4-based SSL (TLS), since SSL generates the encryption keys it uses for RC4 by hashing, meaning that different SSL sessions have unrelated keys.
Weaknesses of WEP

- two-time pad attack: IV is 24 bits long, so the key is reused after at most $2^{24}$ frames
  → use longer IVs

- Fluhrer, Mantin and Shamir (FMS) attack (related keys attack):
  - the keys only differ in the 24 bits IV
  - first bytes of key stream known because standard headers are always sent
  - for certain IVs knowing $m$ bytes of key and keystream means you can deduce byte $m+1$ of key
  → instead of using related IVs, generate IVs using a PRG

Remark

The FMS attack does not apply to RC4-based SSL (TLS), since SSL generates the encryption keys it uses for RC4 by hashing, meaning that different SSL sessions have unrelated keys
Linear Feedback Shift Registers (LFSRs)

\[ K = \{0, 1\} \]

Main data structure: register \( R \) of \( s \) bits

Initialisation: \( R := k \)

Keystream generation: 1-bit output per round

Tap: \( i_1, i_2, \ldots, i_\ell \)

Feedback bit: \( R[i_1] \oplus R[i_2] \oplus \cdots \oplus R[i_\ell] \)

Output bit: \( R[s] + i_1 i_2 i_\ell \)

Broken LFSR-based stream ciphers:

- DVD encryption: CSS (2 LFSRs)
- GSM encryption: A5 (3 LFSRs)
- Bluetooth encryption: E0 (4 LFSRs)
Linear Feedback Shift Registers (LFSRs)

- $\mathcal{K} = \{0, 1\}^s$

Main data structure: register $\mathcal{R}$ of $s$ bits

Initialisation: $\mathcal{R} := k$

Keystream generation: 1-bit output per round

Taps: $i_1, i_2, ..., i_\ell$

Feedback bit: $\mathcal{R}[i_1] \oplus \mathcal{R}[i_2] \oplus \cdots \oplus \mathcal{R}[i_\ell]$

Output bit: $\mathcal{R}[s] + i_1 i_2 i_\ell$

Broken LFSR-based stream ciphers:
- DVD encryption: CSS (2 LFSRs)
- GSM encryption: A5 (3 LFSRs)
- Bluetooth encryption: E0 (4 LFSRs)
Linear Feedback Shift Registers (LFSRs)

- $\mathcal{K} = \{0, 1\}^s$
- Main data structure: register $R$ of $s$ bits

Keystream generation: 1-bit output per round

- taps: $i_1, i_2, \ldots, i_\ell$
- feedback bit: $R[i_1] \oplus R[i_2] \oplus \cdots \oplus R[i_\ell]$
- output bit: $R[s] + i_1 i_2 i_3 \cdots i_\ell$

Broken LFSR-based stream ciphers:
- DVD encryption: CSS (2 LFSRs)
- GSM encryption: A5 (3 LFSRs)
- Bluetooth encryption: E0 (4 LFSRs)
Linear Feedback Shift Registers (LFSRs)

- \( \mathcal{K} = \{0, 1\}^s \)
- Main data structure: register \( R \) of \( s \) bits
- Initialisation: \( R := k \)
Linear Feedback Shift Registers (LFSRs)

- $\mathcal{K} = \{0, 1\}^s$
- Main data structure: register $R$ of $s$ bits
- Initialisation: $R := k$
- Keystream generation: 1-bit output per round
  - taps: $i_1, i_2, \ldots i_\ell$
  - feedback bit: $R[i_1] \oplus R[i_2] \oplus \cdots \oplus R[i_\ell]$
  - output bit: $R[s]$

![Diagram of LFSR]

- Broken LFSR-based stream ciphers:
  - DVD encryption: CSS (2 LFSRs)
  - GSM encryption: A5 (3 LFSRs)
  - Bluetooth encryption: E0 (4 LFSRs)
Linear Feedback Shift Registers (LFSRs)

- $\mathcal{K} = \{0, 1\}^s$
- Main data structure: register $R$ of $s$ bits
- Initialisation: $R := k$
- Keystream generation: 1-bit output per round
  - taps: $i_1, i_2, \ldots, i_\ell$
  - feedback bit: $R[i_1] \oplus R[i_2] \oplus \cdots \oplus R[i_\ell]$
  - output bit: $R[s]$

- Broken LFSR-based stream ciphers:
  - DVD encryption: CSS (2 LFSRs)
  - GSM encryption: A5 (3 LFSRs)
  - Bluetooth encryption: E0 (4 LFSRs)
Content Scrambling System (CSS) uses LFSRs

- **K** = \{0, 1\}

- Data structures: 17-bits LFSR \(R_{17}\) and 25-bits LFSR \(R_{25}\)

- Initialisation:
  \[R_{17} := 1 || K[0-15]\]
  \[R_{25} := 1 || K[16-39]\]

- Keystream generation: 1-byte output per round

![LFSR Diagram](image)
Content Scrambling System (CSS) uses LFSRs

- $\mathcal{K} = \{0, 1\}^{40}$
Content Scrambling System (CSS) uses LFSRs

- $\mathcal{K} = \{0, 1\}^{40}$

- Data structures: 17-bits LFSR ($R_{17}$) and 25-bits LFSR ($R_{25}$)
Content Scrambling System (CSS) uses LFSRs

- $\mathcal{K} = \{0, 1\}^{40}$

- Data structures: 17-bits LFSR ($R_{17}$) and 25-bits LFSR ($R_{25}$)

- Initialisation: $R_{17} := 1||K[0 – 15]$
  $R_{25} := 1||K[16 – 39]$
Content Scrambling System (CSS) uses LFSRs

- \( \mathcal{K} = \{0, 1\}^{40} \)
- Data structures: 17-bits LFSR \((R_{17})\) and 25-bits LFSR \((R_{25})\)
- Initialisation:
  \[ R_{17} := 1||K[0 – 15] \]
  \[ R_{25} := 1||K[16 – 39] \]
- Keystream generation: 1-byte output per round
Weaknesses in CSS

Can be broken in time $2^{17}$. The idea of the attack is as follows:
Weaknesses in CSS

Can be broken in time $2^{17}$. The idea of the attack is as follows:

- Because of structure of MPEG-2, first 20 bytes of plaintext are known
Weaknesses in CSS

Can be broken in time $2^{17}$. The idea of the attack is as follows:

- Because of structure of MPEG-2, first 20 bytes of plaintext are known

- Hence also first 20 bytes of keystream are known
Weaknesses in CSS

Can be broken in time $2^{17}$. The idea of the attack is as follows:

- Because of structure of MPEG-2, first 20 bytes of plaintext are known
- Hence also first 20 bytes of keystream are known
- Given output of 17 bit LFSR, can deduce output of 25 bit LFSR by subtraction
Weaknesses in CSS

Can be broken in time $2^{17}$. The idea of the attack is as follows:

▶ Because of structure of MPEG-2, first 20 bytes of plaintext are known

▶ Hence also first 20 bytes of keystream are known

▶ Given output of 17 bit LFSR, can deduce output of 25 bit LFSR by subtraction

▶ Hence try all $2^{17}$ possibilities for 17 bit LFSR and if generated 25 bit LFSR produces observed keystream, cipher is cracked
Modern stream ciphers

Project eStream: project to “identify new stream ciphers suitable for widespread adoption”, organised by the EU ECRYPT network

→ HC-128, Rabbit, Salsa20/12, SOSEMANUK, Grain v1, MICKEY 2.0, Trivium
Modern stream ciphers

**Project eStream**: project to “identify new stream ciphers suitable for widespread adoption”, organised by the EU ECRYPT network

→ HC-128, Rabbit, Salsa20/12, SOSEMANUK, Grain v1, MICKEY 2.0, Trivium

**Conjecture**

These eStream stream ciphers are “secure”
Concluding remarks

Perfect secrecy does not capture all possible attacks. \( \rightarrow \) need for different security definition

Theorem (Shannon 1949) Let \( (E, D) \) be a cipher over \( (M, C, K) \). If \( (E, D) \) satisfies perfect secrecy, then the keys \( |K| \leq |M| \). \( \Rightarrow \) Stream ciphers do not satisfy perfect secrecy because the keys in \( K \) are smaller than the messages in \( M \). \( \rightarrow \) need for different security definition

The design of crypto primitives is a subtle and error prone task: define threat model, propose construction, prove that breaking construction would solve an underlying hard problem. \( \rightarrow \) use standardised publicly known primitives

Crypto primitives are secure under a precisely defined threat model. \( \rightarrow \) respect the security assumptions of the crypto primitives you use
Concluding remarks

- Perfect secrecy does not capture all possible attacks.
  → need for different security definition
Concluding remarks

- Perfect secrecy does not capture all possible attacks. → need for different security definition

- Theorem (Shannon 1949) Let \((E, D)\) be a cipher over \((\mathcal{M}, \mathcal{C}, \mathcal{K})\). If \((E, D)\) satisfies perfect secrecy, then the keys should be at least as long as the plaintexts \(|\mathcal{K}| \leq |\mathcal{M}|\).
  ⇒ Stream ciphers do not satisfy perfect secrecy because the keys in \(\mathcal{K}\) are smaller than the messages in \(\mathcal{M}\)
  → need for different security definition
Concluding remarks

- Perfect secrecy does not capture all possible attacks.
  → need for different security definition

- Theorem (Shannon 1949) Let $(E, D)$ be a cipher over $(\mathcal{M}, \mathcal{C}, \mathcal{K})$. If $(E, D)$ satisfies perfect secrecy, then the keys should be at least as long as the plaintexts ($|\mathcal{K}| \leq |\mathcal{M}|$).
  ⇒ Stream ciphers do not satisfy perfect secrecy because the keys in $\mathcal{K}$ are smaller than the messages in $\mathcal{M}$
  → need for different security definition

- The design of crypto primitives is a subtle and error prone task: define threat model, propose construction, prove that breaking construction would solve an underlying hard problem.
  → use standardised publicly know primitives
Perfect secrecy does not capture all possible attacks. → need for different security definition

Theorem (Shannon 1949) Let $(E, D)$ be a cipher over $(\mathcal{M}, \mathcal{C}, \mathcal{K})$. If $(E, D)$ satisfies perfect secrecy, then the keys should be at least as long as the plaintexts ($|\mathcal{K}| \leq |\mathcal{M}|$).

⇒ Stream ciphers do not satisfy perfect secrecy because the keys in $\mathcal{K}$ are smaller than the messages in $\mathcal{M}$ → need for different security definition

The design of crypto primitives is a subtle and error prone task: define threat model, propose construction, prove that breaking construction would solve an underlying hard problem. → use standardised publicly know primitives

Crypto primitives are secure under a precisely defined threat model. → respect the security assumptions of the crypto primitives you use