Lecture 3
Introduction

Stream Ciphers:
Attacks

Block Ciphers:
Definitions

DES
Administrative Details

• Course website: 
  https://courses.grainger.illinois.edu/cs498ac3/fa2020/
• Has syllabus, instructor and TA info, office hours
• IMPORTANT: Join Piazza!
  piazza.com/illinois/fall2020/ececs498ac/home

*I strongly encourage class participation.*
*If you don't understand something in class, please interrupt me and ask questions.*
*Please make abundant use of office hours.*
Stream Ciphers: Examples and Attacks
Symmetric Ciphers

• A cipher defined over \((K, M, C)\)
  
is a pair of efficient algorithms \((E, D)\) where
  
  \[
  E: K \times M \rightarrow C \\
  D: K \times C \rightarrow M
  \]
  
  that satisfies –

  **Correctness:** For all \(m \in M, k \in K\), \(D \left( k, E(k, m) \right) = m\)

  **Semantic Security:** for all \(m_0, m_1 \in M\):
  
  \[
  E(k,m_0) \approx_c E(k,m_1)
  \]

  computationally bounded \(ADV \leftrightarrow \text{PPT Turing Machine} \)

  polynomial-sized circuit
Attack: Integrity

In the PRG-based cipher, 

\[ E(k, m) = PRG(k) \oplus m \]

easy to convert \( E(k, m) \rightarrow E(k, m \oplus 1) \) \( (\text{mod } 2) \)

\[ E(k, m) = \underbrace{PRG(k) \oplus m}_{\oplus 000\ldots 1} = PRG(k) \oplus (m \oplus 0\ldots01) \]

\[ \rightarrow E(k, m \oplus 1) \]
Example: RC4 Cipher (deprecated)

- Expand 128-bit seed to 2048 bits of pseudorandomness
- Use pseudorandomness to initialize internal state
- Used in HTTPS, WEP

Weaknesses:

1. Not pseudorandom: e.g. [0,0] appears more often than it should
2. Related key attacks make it possible to recover the key

https://blog.cryptographyengineering.com/2013/03/12/attack-of-week-rc4-is-kind-of-broken-in/
Example: CSS Stream Cipher (badly broken)

- Used to encrypt DVDs. Was designed to be hardware friendly.

- Linear feedback shift register (used in DVD, GSM, bluetooth, all broken)
Example: CSS Stream Cipher (badly broken)

- Seed size = 5 bytes = 40 bits.

1 byte = 8 bits.
Example: CSS Stream Cipher (badly broken)

- Seed size = 5 bytes = 40 bits.
Better Stream Ciphers

• Salsa20/12, Sosemanuk

  Nonce: a non-repeating value for a given key

  \[ E(k, m ; r) = m \oplus PRG(k ; r) \]

  The pair \((k, r)\) is used at most once

• Pseudo random generators in practice: (e.g. /dev/random)

  Continuously add entropy to internal state

  Entropy sources:
  • Timing: hardware interrupts (keyboard, mouse)
Block Ciphers
Block Ciphers

Examples:
1. 3DES: \( n = 64 \) bits, \( k = 168 \) bits
2. AES: \( n = 128 \) bits, \( k = 128, 192, 256 \) bits
Examples:
1. 3DES: $k = 168$ bits, $j = 16$, each $k_j = 48$ bits
2. AES: $k = 128/192/256$ bits, $j = 10$, each $k_j = 128$ bits
Defining Security for Block Ciphers

- A **pseudorandom function (PRF)** is a function from $\mathcal{K} \times \mathcal{X} \rightarrow \mathcal{C}$ s.t. $F(k, m)$ is efficiently computable for every $k$ and $m$

- A **pseudorandom permutation (PRP)** is a function from $\mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$ s.t. $F(k, m)$ is efficiently computable for every $k$ and $m$, and $F(k, \cdot)$ has domain = image and is one-to-one, and $F^{-1}(k, y)$ is efficiently computable for every $k$ and $y$ where $F^{-1}(k, F(k, x)) = x$

AES, DES are PRPs. In AES, $|\mathcal{X}| = 2^{128}$ and in DES, $|\mathcal{X}| = 2^{64}$. 

**Permutation**: $1, 2, ..., N \xrightarrow{\text{perm}} 1, 2, ..., N$

**Random**

$1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 4, ..., N-1 \rightarrow N, N \rightarrow 1$
Defining Security for Block Ciphers

• A **pseudorandom function (PRF)** is a function from $\mathcal{K} \times \mathcal{X} \to \mathcal{C}$
  
  s.t. $F(k, m)$ is efficiently computable for every $k$ and $m$

  and is indistinguishable from a “random” function

\[
\Pr[\hat{a} = 1 | \text{Game 0}] - \Pr[\hat{a} = 1 | \text{Game 1}] < \varepsilon
\]
Question 1

Let $F : K \times X \rightarrow X$ be a secure PRP.

Is $F$ a secure PRF?

1. Always
2. Never
3. Depends on $F$
Question 2

Let \( F: K \times X \rightarrow \{0,1\}^{128} \) be a secure PRF.

Is the following \( F' \) a secure PRF?

\[
F'(k, x) = \begin{cases} 
1^{128} & \text{if } x=0 \\
F(k, x) & \text{otherwise}
\end{cases}
\]

1. Yes
2. No
3. Depends on \( F \)
Question 3

Let \( F: K \times X \rightarrow \{0,1\}^{128} \) be a secure PRF.
Can you build a PRG \( G: K \rightarrow \{0,1\}^{4096} \) from \( F \)?

\[
\text{PRG}(K) = F(K, 0^8) \ || F(K, 0^3) \ || F(K, 0^{10}) \ldots \]

\[
\frac{4096}{128} = \frac{2^{12}}{2^7} = 2^5
\]

Can you build a PRF from a PRG?

(Try on your own!)
DES
Given functions $f_1, \ldots, f_j : \{0,1\}^n \rightarrow \{0,1\}^n$

Build an invertible function $F : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$

$X = (L_0, R_0)$

$L_1 = R_0$

$R_1 = L_0 \oplus f_1(R_0)$

$L_2 = R_1$

$R_2 = L_1 \oplus f_2(R_1)$

$\vdots$

$E(k_1(D(k_2, E(k_3, m))))$
Given functions $f_1, \ldots, f_j : \{0,1\}^n \rightarrow \{0,1\}^n$

Build an invertible function $F : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$

$L_0, R_0 \rightarrow (L_j, R_j)$

\[ R_{j-1} \rightarrow L_j \]

\[ L_{j-1} \rightarrow R_j \oplus f_j(R_{j-1}) \]

\[ R_j \oplus f_j(L_j) \]
PRFs => PRPs

Luby-Rackoff ‘85:
If \( f: K \times \{0,1\}^n \rightarrow \{0,1\}^n \) is a secure PRF
then 3-round Feistel \( F: K^3 \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n} \) is a secure PRP

To prove this, show that:

1. Feistel results in an invertible function, i.e.
2. If each \( f_i \left( \begin{array}{c} f_1 \text{ PRF}(K_1, \cdot) \\
                             f_2 \text{ PRF}(K_2, \cdot) \\
                             f_3 \text{ PRF}(K_3, \cdot) \end{array} \right) \) is a secure PRF,
then so is the Feistel.
DES

DES: $n = 64$ bits, $k = 56$ bits, $j = 16$, each $k_j = 48$ bits
Each function $f_i = F(k_i, x)$ is:
Requirements on S-boxes

- Implemented as lookup tables
- Must **not be** linear functions
- Note that all other functions are linear. If S-boxes are linear, it means that DES encryption can be represented as a matrix

\[
DES(k, m) = \begin{bmatrix}
B \oplus B \\
B \oplus B \\
\end{bmatrix}
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
\end{bmatrix} =
\begin{bmatrix}
m_1 \oplus m_2 \oplus m_3 \\
k \oplus k \oplus k \\
\end{bmatrix}
\]

This is BAD!
Summary

• Block ciphers formalized as pseudorandom permutations (PRPs)

• Feistel Network, DES

• Next time, we will look at AES