Blockcipher

Viet Tung Hoang

Some slides are based on material from Prof. Mihir Bellare (UCSD) and Prof. Stefano Tessaro (UW)
1. Blockciphers
2. Birthday Attack
3. App: TCP Sequence Number
4. App: One-time Password
5. App: Challenge-Response Protocol
Blockcipher

$E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$

efficiently invertible given the key
Random key $K$ is known to both parties, but not given to adversary $A$
Real-world Blockciphers

NIST Special Publication 800-67
Version 1.1

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
Revised 19 May 2008
William C. Barker

3DES, deprecated since 2017 but still in legacy software
\[ k = 168, n = 64 \]

FIPS 197
Federal Information Processing Standards Publication

Advanced Encryption Standard (AES)

Category: Computer Security
Subcategory:

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

AES, national standard
\[ k \in \{128, 192, 256\}, n = 128 \]
# Defining Security for Blockcipher

<table>
<thead>
<tr>
<th>Possible Properties</th>
<th>Necessary</th>
<th>Sufficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard to recover the key</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hard to find $M$ given $C \leftarrow E_K(M)$</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Want**: a single “master” property that is sufficient to ensure security of common usage of blockcipher.
An Analogy: Turing Test

What does it mean for a machine to be “intelligent”?

Possible Answers

<table>
<thead>
<tr>
<th>It can be happy</th>
<th>But no such list is satisfactory</th>
</tr>
</thead>
<tbody>
<tr>
<td>It recognizes pictures</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
An Analogy: Turing Test

Man (0) or Machine (1)?
<table>
<thead>
<tr>
<th>Notion</th>
<th>Real object</th>
<th>Ideal object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence</td>
<td><img src="image1" alt="Robot" /></td>
<td><img src="image2" alt="Person" /></td>
</tr>
<tr>
<td>PRF</td>
<td>$E_K$</td>
<td>Random function</td>
</tr>
</tbody>
</table>
Informal View of PRF Security

\[ E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \]

Sample random \( f : \{0, 1\}^n \rightarrow \{0, 1\}^n \)

\( K \leftrightarrow \mathcal{K} \)

Adversary doesn’t know \( K \) or \( f \)
Defining Random Function: Lazy Sampling

**Want:** a *random* function $f : \{0, 1\}^n \to \{0, 1\}^m$

Pick a fresh random answer for a new query, and remember the answer...
Defining Random Function: Lazy Sampling

**Want:** a random function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$

Pick a fresh random answer for a new query, and remember the answer
Defining Random Function: Lazy Sampling

**Want:** a random function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$

Pick a fresh random answer for a new query, and remember the answer
Defining Random Function: Lazy Sampling

**Want:** a random function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$

Pick a fresh random answer for a new query, and remember the answer
Want: a random function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$
Putting Things in Code

**Game** \( \text{Real}_E \)

**procedure** Initialize()

\[ K \leftrightarrow K \]

**procedure** Fn(M)

return \( E_K(M) \)

**Game** \( \text{Rand}_E \)

string array \( T = \{\} \) // Global variable

**procedure** Fn(M)

If \( T[M] = \perp \) then \( T[M] \leftrightarrow \{0, 1\}^n \)

return \( T[M] \)

\[ \text{Adv}^\text{prf}_E(A) = \Pr[\text{Real}_E^A \Rightarrow 1] - \Pr[\text{Rand}_E^A \Rightarrow 1] \]
Exercise: PRF Attacks

\[ E_K(M) = M \oplus K \]

\[ E_K(M) = AES_K(M) \parallel AES_K(\overline{M}) \]
1. Blockciphers

2. Birthday Attack

3. App: TCP Sequence Number

4. App: One-time Password

5. App: Challenge-Response Protocol
Birthday Problem

$C(N, q) = \Pr[y_1, \ldots, y_q \text{ not distinct}]$

**Fact:** For $q \leq \sqrt{2N}$,

$$\frac{q(q-1)}{4N} \leq C(N, q) \leq \frac{q(q-1)}{2N}$$
Birthday Attack on PRF Security

distinct $M_1, \ldots, M_q$

\[ E_K \]

distinct $C_1, \ldots, C_q$

distinct $M_1, \ldots, M_q$

\[ f \]

random $C_1, \ldots, C_q$
Birthday Attack on PRF Security

\[ E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \]

Output 1 if \( C_1, \ldots, C_q \) are distinct

\[ \text{Adv}^\text{prf}_E (A) = C(2^n, q) \approx \frac{q^2}{2^n} \]

Need \( 2^{n/2} \) queries to break PRF security

<table>
<thead>
<tr>
<th>Blockcipher</th>
<th>( n )</th>
<th>( 2^{n/2} )</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>64</td>
<td>( 2^{32} )</td>
<td>Insecure</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>( 2^{64} )</td>
<td>Secure</td>
</tr>
</tbody>
</table>
Does It Matter In Practice?

Sweet32: Birthday Attacks on 64-bit Blockciphers in TLS and OpenVPN

[References: Bhargavan, Leurent 16]

HTTPS encryption via 3DES

Recover cookie after capturing 785GB
Agenda

1. Blockciphers
2. Birthday Attack
3. App: TCP Sequence Number
4. App: One-time Password
5. App: Challenge-Response Protocol
TCP Recap

- Handshake
- Session data
- Termination
TCP Handshake

SYN: Alice’s Seq # is $X$

ACK: Your Seq # is $X$

SYN: Server’s Seq # is $Y$

ACK: Your Seq # is $Y$
The Use of Sequence Numbers

Set up Seq # as 3001

Can still reorder out-of-order packets
Security Issue: Denial-of-Service Attack

Session data

Need to guess seq #, but it’s easy in early TCP implementations

Reset, source=Alice
Security Issue: Connection Spoofing

**SYN:** Alice’s Seq # is \( X \),
source IP = Alice

**ACK:** Your Seq # is \( X \)

**SYN:** Server’s Seq # is \( Y \)

**ACK:** Your Seq # is \( Y \)

Now execute command on Alice’s behalf
First Attempt: Random Sequence Number
Backward Compatibility Issue

Requirement: If two connections of same IP addresses and ports are within a small window, must have $X < Y$ to avoid interference from delayed packets
Generating TCP Sequence Numbers with PRF

Port 1234, IP A

|\[ T \]
|\[ K \]

Not shared with Alice

Server’s Seq # = \( T + F_K(A\|1234\|S\|80) \)
Agenda

1. Blockciphers
2. Birthday Attack
3. App: TCP Sequence Number
4. App: One-time Password
5. App: Challenge-Response Protocol
Motivation

Goal: An eavesdropper cannot later open the car
A Wrong Solution

“Open the door”

Question: Why is it bad?
One-Time Password Via PRF


Should allow time drift, and accept for slightly outdated time

(Stateful) alternative: Run the PRF on a synchronized counter

A Real-world Example: RSA’s SecureID

But it’s disastrous if the key is stolen

SecurID breach cost RSA $66m

In 2nd quarter alone

Dan Goodin  Wed 27 Jul 2011 // 17:17 UTC
1. Blockciphers
2. Birthday Attack
3. App: TCP Sequence Number
4. App: One-time Password
5. App: Challenge-Response Protocol
Motivation: Man-In-The-Middle Attack

Question: Does one-time password work here?
Solution: Challenge-Response

Nonce: a string that should never repeat