Cryptography Basics and Symmetric Cryptography

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 2

ravi.utsa@gmail.com
www.profsandhu.com
Basic Concepts
Cryptographic Technology

SYMMETRIC KEY
Secret Key
Single Key
Conventional

ASYMMETRIC KEY
Public Key
Public-Private Key
Cryptographic Technology

- Symmetric-key encryption
- Symmetric-key message authentication codes (MACs)
- Public-key encryption
- Public-key digital signatures
- Public-key key agreement
- Message digests (hash functions)
- Public-key certificates
- Challenge-response authentication
Symmetric-key encryption
Symmetric-key message authentication codes (MAC)
Public-key encryption
Public-key digital signatures
Public-key key agreement
Message digests (hash functions)
Public-key certificates
Challenge-response authentication

SSL uses all of these

ATMs run on symmetric-key technology
Cryptographic Services

- confidentiality
  - traffic flow confidentiality
- integrity
- authentication
- non-repudiation

Traditional formulation
Cryptographic Services

- confidentiality
  - crypto keys leak profusely via side channels
- integrity + authentication
  - no point having one without the other
- non-repudiation
  - requires asymmetric cryptography
  - stronger form of integrity + authentication
- replay protection
  - beyond integrity?

Important insights
Symmetric-key cryptography
- 128 bit or higher

Public-key cryptography
- 2048 bit or higher

Message digests
- 256 bit or higher

These numbers keep increasing
- https://www.keylength.com/
Symmetric Encryption
Symmetric-Key Encryption

**INSECURE CHANNEL**

A

Encryption Algorithm E

Ciphertext

B

Decryption Algorithm D

Plain-text

**SECURE CHANNEL**

Confidentiality
Integrity

K

Symmetric Key shared by A and B

K

© Ravi Sandhu

World-Leading Research with Real-World Impact!
- Confidentiality depends only on secrecy of the key
  - Size of key is critical
- Symmetric key systems do not scale well
  - With N parties, we need to generate and distribute $N(N-1)/2$ keys
- A and B can be people or computers
Master Keys and Session Keys

- master keys, long lifetime
  - prolonged use increases exposure
- session keys
  - short-term keys communicated by means of
    - master symmetric keys
    - public key technology
Cryptanalysis

- ciphertext only
  - cryptanalyst only knows ciphertext
- known plaintext
  - cryptanalyst knows some plaintext-ciphertext pairs
- chosen plaintext
- chosen ciphertext
40 bit key requires $2^{39} \approx 5 \times 10^{11}$ trials on average (exportable from USA, early 1990’s)

trials/second time required

<table>
<thead>
<tr>
<th>trials/second</th>
<th>time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20,000 years</td>
</tr>
<tr>
<td>$10^3$</td>
<td>20 years</td>
</tr>
<tr>
<td>$10^6$</td>
<td>6 days</td>
</tr>
<tr>
<td>$10^9$</td>
<td>9 minutes</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>0.5 seconds</td>
</tr>
</tbody>
</table>
56 bit key requires $2^{55} \approx 3.6 \times 10^{16}$ trials on average (DES, 1977)

<table>
<thead>
<tr>
<th>Trials/second</th>
<th>Time Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^9$ years</td>
</tr>
<tr>
<td>$10^3$</td>
<td>$10^6$ years</td>
</tr>
<tr>
<td>$10^6$</td>
<td>$10^3$ years</td>
</tr>
<tr>
<td>$10^9$</td>
<td>1 year</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>10 hours</td>
</tr>
</tbody>
</table>
80 bit key requires $2^{79} \approx 6 \times 10^{23}$ trials on average (SKIPJACK, mid-1990s)

trials/second time required

<table>
<thead>
<tr>
<th>Trials/second</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^{16}$ years</td>
</tr>
<tr>
<td>$10^3$</td>
<td>$10^{13}$ years</td>
</tr>
<tr>
<td>$10^6$</td>
<td>$10^{10}$ years</td>
</tr>
<tr>
<td>$10^9$</td>
<td>$10^7$ years</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>$10^4$ years</td>
</tr>
</tbody>
</table>
128 bit key requires $2^{127} \approx 2 \times 10^{38}$ trials on average (AES-128, 2001)

trials/second time required

<table>
<thead>
<tr>
<th>Trials/Second</th>
<th>Time Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^{30}$ years</td>
</tr>
<tr>
<td>$10^3$</td>
<td>$10^{27}$ years</td>
</tr>
<tr>
<td>$10^6$</td>
<td>$10^{24}$ years</td>
</tr>
<tr>
<td>$10^9$</td>
<td>$10^{21}$ years</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>$10^{18}$ years</td>
</tr>
</tbody>
</table>
AES

- Advanced encryption standard, 2001
  - DES, 1977: designed by IBM. Blessed by NSA.
  - SKIPJACK, early 1990s: designed by NSA, declassified 1998
  - AES, 2001: designed by open international competition, winner was a European team
- 3 key sizes: 128, 192, 256
- Block size: 128
  - Previously most (e.g. DES) used 64 bit block size
  - 128 bit block size is safer due to birthday attack
Symmetric-Key Encryption

INSECURE CHANNEL

Plain-text

Encryption Algorithm E

Ciphertext

Decryption Algorithm D

Plain-text

A

Symmetric Key shared by A and B

K

B

SECURE CHANNEL
Confidentiality
Integrity
Password Derived Keys

INSECURE CHANNEL

Plain-text

Encryption Algorithm E

Ciphertext

Decryption Algorithm D

Plain-text

Symmetric Key
shared by A and B

Key Derivation Function

Password (salted)

Key Derivation Function

Password (salted)
Password Derived Keys

Plain-text

INSECURE CHANNEL

Encrypting Algorithm E

Ciphertext

Decrypting Algorithm D

Plain-text

Symmetric Key

shared by A and B

A

K

Key Derivation Function

Password (salted)

Dictionary attack

B

K

Key Derivation Function

Password (salted)

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Perfect Secrecy

Plain-text \rightarrow + \rightarrow \text{Ciphertext} \rightarrow + \rightarrow \text{Plain-text}

Mi \rightarrow + \rightarrow Ci \rightarrow + \rightarrow Mi

Symmetric Key \rightarrow Ki \rightarrow Ki

Vernam one-time pad

A B A\oplus B
0 0 0
0 1 1
1 0 1
1 1 0

SECURE CHANNEL
Double DES

- effective key size is only 57 bits due to meet-in-the-middle attack

X Not covered in lecture

Not covered in lecture
Triple DES

- effective key size is 112 bits due to meet-in-the-middle attack

Not covered in lecture
Electronic Code Book (ECB) Mode

- OK for small messages
- Identical data blocks will be identically encrypted
Cipher Block Chaining (CBC) Mode

- **128 bit Data block**
- **128 bit key**
- **⊕ is the exclusive OR operation**
- **128 bit previous ciphertext block**
- **128 bit Data block**
- **128 bit key**
Symmetric-Key Message Authentication Code (MAC)
Message Authentication Code

INSECURE CHANNEL

Plain-Text → MAC Algorithm M → Verification Algorithm V → Yes/No

plaintext + MAC

Plain-Text

A

K

B

K
Message Authentication Code

INSECURE CHANNEL

Plain-text → MAC Algorithm M → Plaintext + MAC

Verification Algorithm V

Yes/No

K

Does not provide non-repudiation

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Message Authentication Code

- Symmetric Encryption Based
- Message-Digest Based
Message Authentication Code

Symmetric Encryption Based

Message-Digest Based

Will revisit after discussing message digests