Encryption

Tom Chothia
Computer Security: Lecture 2
Encryption 1

• Secure symmetric key encryption:
  – One time pads
  – AES, DES and 3-DES

• Block cipher modes

• Truecrypt
Xor $\oplus$

$(M \oplus k) \oplus k = M$

<table>
<thead>
<tr>
<th></th>
<th>xor 0 = 0</th>
<th>xor 1 = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Hello Alice

```
01011001 01100101 01110011
```

Key

```
11001011 01001101 11110001
```

```
10010010 00101000 10000010
```

$\oplus$

ascii

```
01011001 01100101 01110011
```

$\oplus$

```
10010010 00101000 10000010
```
Xor \quad \oplus \\

(M \oplus k) \oplus k = M \\

Hello Alice \quad \text{ascii} \\
11001011 01001101 11110001 \\
01011001 01100101 01110011 \\
11001011 01001101 11110001 \\
10010010 00101000 10000010 \\

0 \text{ xor } 0 = 0 \\
1 \text{ xor } 0 = 1 \\
0 \text{ xor } 1 = 1 \\
1 \text{ xor } 1 = 0
## Vigenere Table

<table>
<thead>
<tr>
<th>KEY</th>
<th>ABCDEFGHIJKLMNOPQRSTUVWXYZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A B C D E F G H I J K L M N O P Q R S T U V W X Y Z</td>
</tr>
<tr>
<td>B</td>
<td>B C D E F G H I J K L M N O P Q R S T U V W X Y Z A</td>
</tr>
<tr>
<td>D</td>
<td>D E F G H I J K L M N O P Q R S T U V W X Y Z A B C</td>
</tr>
<tr>
<td>E</td>
<td>E F G H I J K L M N O P Q R S T U V W X Y Z A B C D</td>
</tr>
<tr>
<td>F</td>
<td>F G H I J K L M N O P Q R S T U V W X Y Z A B C D E</td>
</tr>
<tr>
<td>G</td>
<td>G H I J K L M N O P Q R S T U V W X Y Z A B C D E F</td>
</tr>
<tr>
<td>H</td>
<td>H I J K L M N O P Q R S T U V W X Y Z A B C D E F G</td>
</tr>
<tr>
<td>I</td>
<td>I J K L M N O P Q R S T U V W X Y Z A B C D E F G H</td>
</tr>
<tr>
<td>J</td>
<td>J K L M N O P Q R S T U V W X Y Z A B C D E F G H I</td>
</tr>
<tr>
<td>K</td>
<td>K L M N O P Q R S T U V W X Y Z A B C D E F G H I J</td>
</tr>
<tr>
<td>L</td>
<td>L M N O P Q R S T U V W X Y Z A B C D E F G H I J K</td>
</tr>
<tr>
<td>M</td>
<td>M N O P Q R S T U V W X Y Z A B C D E F G H I J K L</td>
</tr>
<tr>
<td>N</td>
<td>N O P Q R S T U V W X Y Z A B C D E F G H I J K L M</td>
</tr>
<tr>
<td>O</td>
<td>O P Q R S T U V W X Y Z A B C D E F G H I J K L M N</td>
</tr>
<tr>
<td>P</td>
<td>P Q R S T U V W X Y Z A B C D E F G H I J K L M N O</td>
</tr>
<tr>
<td>Q</td>
<td>Q R S T U V W X Y Z A B C D E F G H I J K L M N O P</td>
</tr>
<tr>
<td>R</td>
<td>R S T U V W X Y Z A B C D E F G H I J K L M N O P Q</td>
</tr>
<tr>
<td>T</td>
<td>T U V W X Y Z A B C D E F G H I J K L M N O P Q R S</td>
</tr>
<tr>
<td>U</td>
<td>U V W X Y Z A B C D E F G H I J K L M N O P Q R S T</td>
</tr>
<tr>
<td>V</td>
<td>V W X Y Z A B C D E F G H I J K L M N O P Q R S T U</td>
</tr>
<tr>
<td>W</td>
<td>W X Y Z A B C D E F G H I J K L M N O P Q R S T U V</td>
</tr>
<tr>
<td>X</td>
<td>X Y Z A B C D E F G H I J K L M N O P Q R S T U V W</td>
</tr>
<tr>
<td>Z</td>
<td>Z A B C D E F G H I J K L M N O P Q R S T U V W X Y</td>
</tr>
</tbody>
</table>
One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Message: HELLOALICE
Key: SGFKPQYEIJ
Cipher text: ALRWERKNLO
One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text: ALRWERKNLO
Key: SGFKPQYEIJ
Message: HELLOALICE
One Time Pads

- Perfect encryption
- Needs a key as long as the message.
- XOR/add the key and the message:

Cipher text: ALRWERKNLO
Key: TWCSCTFLWM
Message: GOODBYEBOB
One Time Pads

• Problem
  – The key needs to be as long as the message.

• Russia during and after W.W.2
  – Reused the key material
  – Broken by the Venona project.
Block Ciphers

• Modern ciphers work on blocks of plain text, not just a single symbol.

• They are made up of a series of permutations and substitutions repeated on each block.

• The key controls the exact nature of the permutations and substitutions.
Advanced Encryption Standard (AES)

- AES is a state-of-the-art block cipher.
- It works on blocks of 128-bits.
- It generates 10 round keys from a single 128-bit key.
- It uses one permutation: ShiftRows and three substitutions SubBytes, MixColumns, AddRoundKey.
Modulo Arithmetic

• Arithmetic modulo “n” means that you count up to “n-1” then loop back to 0
• i.e., 0,1,2,...,n-1,0,1,2,...,n-1,0,1,2,...

• \( a \mod b = r \) for largest whole number \( k \) such that \( a = b.k + r \)

• e.g. \( 9 \mod 4 = 1 \) because \( 9 = 2.4 +1 \)
• The “SubByte” is a fixed substitution based on matrix multiplication, one byte at a time.
“ShiftRows” moves the
- 2nd row one byte to the left,
- the 3rd row two bytes
- and the 4th row 3 bytes.
“MixColumn” is a substitution of each column such that:

\[
(a_0.x^3 + a_1.x^2 + a_2.x + a_3) \times (a_0.x^3 + a_1.x^2 + a_2.x + a_3) \mod (x^4+1) = (b_0.x^3 + b_1.x^2 + b_2.x + b_3)
\]
- "AddRoundKey" xor’s the block with the 128-bit round key (which was generated from the main key).

- \( b_{i,j} = a_{i,j} \text{ xor } k_{i,j} \)
AES

• AES encrypts data by first generating the round keys from the main key
• Then 9 rounds of:
  1. SubBytes
  2. ShiftRows
  3. MixColumns
  4. AddRoundKey
• Finally:
  1. SubBytes
  2. ShiftRows
  3. AddRoundKey
DES

The Data Encryption Standard (DES), was the previous standard.

Designed by IBM in early 1970’s

Before it was accepted as a standard the NSA stepped in and added S-boxes and fixed the key length at 56 bits
S-boxes are a type of substitution.

It was unclear at the time why the NSA added S-boxes to the design.

Many believed these were a back door for the NSA.
DES

- In 1990, Biham & Shamir discovered differential cryptanalysis.

- The S-boxes had made DES resistant to differential cryptanalysis.

- It seems that the NSA knew about differential cryptanalysis, at the start of the 1970s and had step into to protect DES.
Cost to Break DES

• 1977, Diffie and Hellman, theoretically: $20 million, break in 1 day.
• 1993, theoretically $1 million, in 7 hours.
• 1997, RSA Security offer $10,000 for a real break,
  – won by a distributed computing project, at “no cost”
  – EFF (Electronic rights group) break in 56 hours for $250,000
• 2006, COPACOBANA, general purpose brute force, break DES for $10,000
A word about key length

**A Crypto Nerd's Imagination:**

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

**What Would Actually Happen:**

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.

Source:
3-DES

- Tripe DES, was a stop gap until AES
- 3-DES takes 3 keys, $K_1$, $K_2$ & $K_3$.
  $E_{K_1K_2K_3}(M) = E_{K_3}(D_{K_2}(E_{K_1}(M)))$
- Setting $K_1=K_2=K_3$ gives you DES
- Expected to be good until 2030
- Used in bank cards and RFID chips
Block Cipher Modes

• Block Ciphers can be used in a number of modes:

• 1) Electronic codebook mode (ECB)
  – each block is encrypted individually,
  – encrypted blocks are assembled in the same order as the plain text blocks.
  – if blocks are repeated in the plain text, this is revealed by the cipher text.
Block Cipher Modes

Original  ECB
Block Cipher Modes

2) Cipher Block Chaining mode (CBC)
   – each block XOR'd with previous block
   – start with a random Initialization Vector (IV)
   – helps overcome replay attack.

• Suppose the plain text is $B_1, B_2, \ldots, B_n$.
  IV = random number (sent in the clear)
  $C_1 = \text{encrypt}(B_1 \text{ xor IV})$,
  $C_2 = \text{encrypt}(B_2 \text{ xor } C_1)$.
  \ldots $C_i = \text{encrypt}(B_i \text{ xor } C_{i-1})$. 
Block Cipher Modes

Cipher Block Chaining (CBC) mode encryption
Block Cipher Modes

Original       ECB       CBC
TrueCrypt

• TrueCrypt is state-of-the-art encryption software.

• It allows you to create encrypted partition on your harddrive/USB stick

• See demo.
Encryption 1

- Symmetric Key Encryption Ciphers
  - Frequency Analysis
  - One time pads
  - AES, DES and 3-DES

- Block cipher modes

- Truecrypt
Next Lecture

- More on Cipher Block Modes.

- The Diffie Hellman Protocol

- Public Key Encryption
  - RSA
  - Signing