## 

## [3413ICT Network Security](file:///C:\Documents%20and%20Settings\s995689\My%20Documents\Teaching\Courses_2013\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 2B**

**Part 1 – Reviewing the lecture notes, answer the following questions**

1. Explain the difference between diffusion and confusion.

Diffusion: Dissipates statistical structure of plaintext over bulk of cipher text  
Confusion: Makes the relationship between key and cipher text as confusing as possible.

1. Many symmetric block ciphers use a similar structure as the Feistel Cipher. Explain the structure and operation of the Feistel cipher.

Takes a block of 64 bits and encrypts using a 56 bit key. A product cipher that implements Shannon’s concepts of diffusion and confusion. Data is partitioned into two blocks (a left and right) where a substitution takes places on the left based on the right block and a sub key. This process is continued through multiple rounds.

1. Compare DES and AES in terms of data-block length and key size. Explain why AES is more secure than DES.

DES has a data-block size of 56 bits, AES has a data-block size of 128 bits. The key size of DES is 64 bits for DES, AES has a minimum key size of 128 bits. AES is more secure because of the larger data size and key size

**Part 2 – Challenge Exercises**

The following procedures of key generation and data encryption are part of the first round of the DES encryption and key generation (Please note that the procedures have been simplified). Study the procedures and answer the following questions:

**Key Generation:**

1. Given akey stream, ***K0***, of 64 bits, the following bits are stripped: 8th bit, 16th bit, 24th bit, 32nd bit, 40th bit, 48th bit, 56th bit, and 64th bit. A sequence of 56 bits is then obtained.
2. Split the obtained bit sequence into two halves, denoted by *L* and *R*, respectively.
3. Then, let all bits in *L* and *R* rotate left by 1 position (that is, shift circularly to the left by 1 position).
4. Next, pull both rotated *L* and *R* togetherand pass it through the following permutation and contraction:

(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56)

(14,17,11,24,1,5,3,28,15,6,21,10,23,19,12,4,26,8,16,7,27,20,13,2,41,52,31,37,47,55, 30,40,51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32).

Note that in Step (4), not only the bits have been permuted, but also the sequence of 56 bits has been contracted into 48 bits.

By the four steps, we obtain a key, ***K***, which is a sequence of 48 bits.

**Data Encryption:**

1. Given a data block of 32 bits, denoted by ***M***, by the following procedure it is expanded to a sequence of 48 bits:

(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32)

(32,1,2,3,4,5,4,5,6,7,8,9,8,9,10,11,12,13,12,13,14,15,16,17,16,17,18,19,20,21,20,21, 22,23,24,25,24,25,26,27,28,29,28,29,30,31,32,1)

1. The obtained sequence, denoted by ***M\****, is encrypted by the following XOR operation:

******

1. The result of the XOR operation is the ciphertext, denoted by ***C***.

**Answer the following questions:**

1. Suppose you are given the following message and key stream, what is the ciphertext?

***M***= (10011101001110000111100100011111)

***K0 =*** (001110101110101100001111111100001010111101010001111001010 0011010)  
  
(Strip the 8th,16th,24th, 32th, 40th, 48th, 56th, 64th bits)  
0011 101**0** 1110 101**1** 0000 111**1** 1111 000**0** 1010 111**1** 0101 000**1** 1110 010**1** 0001 101**0**  
  
= 0011 1011 1101 0100 0011 1111 1000 1010 1110 1010 0011 1001 0000 1101  
  
L= [0111 0101 1010 1100 0111 1111 0000] R= [0101 1111 0100 0111 0010 1001 1010]  
Lshift = 1110 1011 0101 1000 1111 1110 0000  
Rshift= 1011 1110 1000 1110 0101 0011 0100  
(Combine Left and Right)  
=1110 1011 0101 1000 1111 1110 0000 1011 1110 1000 1110 0101 0011 0100  
 4 8 12 16 20 24 28 32 36 40 44 48 52 56  
(Permute the bits)  
=0100 1110 0011 1110

(**14,17**,**11**,**24**,**1,5**,**3,28**,**15**,**6**,**21**,**10**,**23**,**19**,**12**,**4**,26,8,16,7,27,20,13,2,41,52,31,37,47,55, 30,40,51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32).

(14,17,11,24,1,5,3,28,15,6,21,10,23,19,12,4,26,8,16,7,27,20,13,2,41,52,31,37,47,55, 30,40,51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32).

1. Given the following ciphertext

***C***= (001101001110000110000010011100101000111101001100).

Suppose you know the original message which is

***M***= (11010101101110100101101110011100)

What is the key stream ***K0***?

***M*** = 11010101101110100101101110011100

***K****0* ***=*** 11100001010110111101100111101110

C = 001101001110000110000010011100101000111101001100

**Part 3 – Exercises with CrypTool**

1. Using the Rijndael algorithm, an AES cipher encrypts the plaintext with a number of rounds. In each round, each data block (which consists of 4 groups of 4 bytes) will be processed by the following four operations:
   * Byte substitution
   * Shift rows
   * Mix columns
   * Add round key

Using the Visualization of Algorithms of CrypTool, study how these four operations work.

(Hints: CrypTool 🡪 Indiv. Procedures 🡪Visualization of Algorithms 🡪 AES 🡪 Rijndael Animation)

1. In the hexadecimal notation, each of **0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F** can be translated into a binary sequence of 4 bits as follows:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 9 | A | B | C | D | E | F |
| 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |

So, “AB CD 12 34 EF 89 BC 10 23 AC 56 DE AF 35 ED 36” exactly represent 128 bits. Using the AES cipher with the CrypTool and the key “AB CD 12 34 EF 89 BC 10 23 AC 56 DE AF 35 ED 36”, encrypt the following message:

In [cryptography](http://en.wikipedia.org/wiki/Cryptography), the Advanced Encryption Standard (AES) is a [symmetric-key](http://en.wikipedia.org/wiki/Symmetric-key_algorithm) [encryption](http://en.wikipedia.org/wiki/Encryption) standard adopted by the [U.S. government](http://en.wikipedia.org/wiki/Federal_government_of_the_United_States). The standard comprises three [block ciphers](http://en.wikipedia.org/wiki/Block_cipher), AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with [key](http://en.wikipedia.org/wiki/Key_(cryptography)) sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the [Data Encryption Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES).

And then use the same key to decrypt the ciphertext.