CSS322 – Quiz 2

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 2 December 2010
CSS322Y10S2Q02, Steve/Courses/CSS322/Assessment/Quiz2.tex, r1541

Question 1 [2 marks]

The DES encryption operation, which has 16 rounds, can be written as:

$$ciphertext = IP^{-1}\left(f_{K_{16}}\left(SW\left(f_{K_{15}}\left(SW\left(\ldots\left(f_{K_2}\left(SW\left(f_{K_1}\left(IP\left(plaintext\right)\right)\right)\right)\right)\right)\right)\right)\right)\right)$$

where IP is an initial permutation, f_{K_x} is a round function using key K_x and SW is a switch operation. Write an equation for the DES decryption operation.

Answer. *DES decryption follows the same steps as encryption (i.e. the algorithm is the same) however the keys are used in the opposite order.*

$$plaintext = IP^{-1}\left(f_{K_1}\left(SW\left(f_{K_2}\left(SW\left(\ldots\left(f_{K_{15}}\left(SW\left(f_{K_{16}}\left(IP\left(ciphertext\right)\right)\right)\right)\right)\right)\right)\right)\right)\right)$$

Question 2 [3 marks]

(a) DES is no longer recommended for use today because:

i. **The key space is too small**
ii. The S-Boxes are considered insecure
iii. The avalanche effect is not present
iv. There are not enough rounds

(b) DES is no longer recommended for use today because:

i. Practical timing attacks are possible against it
ii. The avalance effect is not present
iii. **The key length is too short**
iv. The block size is too short

(c) An ideal n-bit block cipher would have:

i. $2n$ possible different plaintext blocks
ii. $2^n!$ possible different plaintext blocks
iii. 2^n possible keys (or transformations)
iv. $2^n!$ **possible keys (or transformations)**

(d) A meet-in-the-middle attack on a Double-DES cipher:

i. Requires an average of approximately 2^{112} operations

ii. **Involves storing approximately 2^{56} blocks in memory to work in practice**

iii. Requires the attacker to know more than 2^{40} plaintext/ciphertext pairs to work in practice

iv. Does not involve applying a brute-force attack on (single) DES

(e) An ideal 4-bit block cipher would have:

i. 16 possible keys (or transformations)

ii. **16! possible keys (or transformations)**

iii. 8 possible different plaintext blocks

iv. 16! possible different plaintext blocks

Question 3 [3 marks]

(a) The Feistel structure for block ciphers achieves security by using multiple rounds, where in each round it alternates between *substitutions* and *transpositions*.

(b) The concept of *diffusion* in block ciphers aims to reduce the statistical nature of input plaintext in the output ciphertext.

(c) Two commonly used block ciphers today are 3DES and *AES or Blowfish or Twofish*.

(d) A *stream* cipher is well suited for real-time encryption, whereas a *block* cipher is better suited for encrypting files.

(e) Techniques that hide messages in fake messages in order to avoid others knowing secret communications are taking place are referred to as *steganography*.

(f) The classical rails fence and rows/column ciphers are known as *transposition* ciphers.

Question 4 [2 marks]

If the initial permutation, IP, of S-DES was [`[3 7 8 1 5 6 2 4]` | `[2 8 7 5 3 4 6 1]`] then IP^{-1} would be:

Answer. *If you apply IP on a sequence of input bits and then apply IP^{-1} on the output then you must obtain the original input bits. If the input bits are:*

`[1 2 3 4 5 6 7 8]`

and IP is:

`[3 7 8 1 5 6 2 4]`

then the 1st bit of the input would become the 4th bit after IP. Therefore after applying IP^{-1} the 4th bit must become the 1st bit. Hence IP^{-1} is:

`[4 7 1 8 5 6 2 3]`

Similarly, if IP is `[2 8 7 5 3 4 6 1]` *then IP^{-1} is* `[8 1 5 6 4 7 3 2]`.