Name ..... ID ..... Section ..... Seat No .....

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2012

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Friday 21 December 2012; 13:30–16:30

Instructions:

- This examination paper has 16 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).

Question 1 [7 marks]

The original IEEE 802.11 wireless LAN protocol used Wired Equivalent Privacy (WEP) for data confidentiality. WEP requires a b-bit secret key, K, shared by sender and receiver (e.g. laptop and access point). For every packet containing n Bytes of data to be sent, WEP concatenates a 24-bit initialisation vector, IV, with the key K, and uses the resulting value as the input to the stream cipher RC4. A n Byte keystream, s, is generated by RC4, which is then used to encrypt the packet. For each new packet, RC4 is applied again, using the same K but different IV (it is incremented by 1 for each packet) to generate a new keystream. The keystream generation can be written as: $s = RC4(K||IV, n)$. The IV is not secret; it is sent, unencrypted, in the header of the corresponding packet.

The operation RC4(*input*, n) can be summarised as:

- Initialise state and temporary vectors based upon *input*
- Perform initial permutation on state vector
- Loop n times: in each loop permutate the state vector and generate a byte of the keystream.

(a) Write an equation for the WEP encryption. That is, given plaintext P (the packet data) as input, how is ciphertext C calculated? Use the variables/notation from the above description. Hint: your answer may include s. [1 mark]

(b) Consider if WEP did not use an IV. Instead, for each packet, RC4 is applied using K as input and producing s as output. Assume RC4(K, n) is applied for each packet and that all packets are the same length. In this case, WEP would be considered very weak. This is because if an attacker can capture just two packets (containing ciphertext) and find a value which is equivalent to the XOR of two plaintexts, i.e. $P_1 \oplus P_2$, assuming the plaintexts are structured (e.g. English messages) then it is relatively easy to find the values of P_1 and P_2. Hence the challenge for the attacker is to find $P_1 \oplus P_2$. Explain how the attacker can find $P_1 \oplus P_2$. [3 marks]

(c) Explain how the use of a 24-bit IV makes the trivial attack from part (b) more difficult. Hint: consider how many packets need to be captured. [2 marks]

(d) WEP has other, related problems, which has meant a new protocol has been developed for wireless LANs called WiFi Protected Access (WPA). WPA uses AES instead of RC4. What is a disadvantage of using AES compared to RC4? [1 mark]

Question 2 [5 marks]

Consider a block cipher, *Double-ABC*, which involves applying the block cipher *ABC* two times (e.g. encrypt the plaintext to obtain a temporary value, then encrypt the temporary value to obtain the ciphertext), each time using a potentially different 3-bit key. The cipher *ABC* is defined by Table 1. The table gives the ciphertext C (columns 2 to 9) produced when encrypting the plaintext P (column 1) with one of the eight keys.

Table 1: ABC Block Cipher

P	K=000	K=001	K=010	K=011	K=100	K=101	K=110	K=111
0000	0001	1001	1010	1010	1100	0111	0011	0001
0001	1011	1100	1001	0011	0000	1000	0001	1100
0010	1111	0000	0010	1011	1101	1111	1101	1011
0011	1000	1000	1110	1000	0101	0010	0000	0100
0100	0000	1101	1111	0111	0001	0011	1011	1000
0101	0111	0010	0011	1001	1111	0101	1100	0101
0110	0010	1110	1000	0000	1110	0000	1010	1010
0111	0011	0101	0000	1100	1010	0110	0111	0011
1000	0100	1011	0111	1101	1011	1110	1110	0110
1001	0101	1111	1101	0100	0100	0100	0100	1110
1010	1010	0110	0100	0110	0011	1101	0101	0000
1011	0110	0100	0110	0101	0111	1010	1111	1001
1100	1110	0011	0101	1111	0110	1001	1000	1111
1101	1101	0111	0001	0010	0010	1011	0110	0111
1110	1100	1010	1011	0001	1001	1100	0010	0010
1111	1001	0001	1100	1110	1000	0001	1001	1101

(a) What is the plaintext when decrypting ciphertext `0011` using key `100111` using *Double-ABC*? [1 mark]

(b) You, as an attacker, have discovered the following past plaintext-ciphertext pairs that two users generated using *Double-ABC* and some key K. Find the key using a meet-in-the-middle attack. [4 marks]

- $P_1 = 0110, C_1 = 0100$
- $P_2 = 1111, C_2 = 1101$

Key: _____

(space for calculating key is below; write your final answer on previous page)

Question 3 [4 marks]

(a) Consider the cipher ABC (Table 1) being used in Counter Mode to act as a pseudorandom number generator. If the initial value of the counter is 0 (decimal) and the seed is 3 (decimal), then what are the first 12 pseudorandom bits? [3 marks]

Bits: _____

(b) What is the maximum period, in bits, of the above PRNG? [1 mark]

Question 4 [12 marks]

(a) The one-time pad is considered to be *unconditionally secure*. What does unconditionally secure mean? [1 mark]

(b) Explain the weakness of the Vigenère cipher. [1 mark]

(c) If a cryptanalyst knows only the encryption algorithm being used, ciphertext, and plaintext chosen by the cryptanalyst together with its corresponding encrypted ciphertext, then an attack can be classified as what type? [1 mark]

(d) Consider the following commands run in Linux (and assume no errors in running the commands):

```
$ echo -n "stevengordonabcd" > file1.txt
```

```
$ openssl enc -aes-256-ofb -in file1.txt -out file2.txt -nopad
-K f27036fbb28e554d6b3a5d8ae68e6423 -iv fd8a418a301fdca8ffa9f8e7305e60df
```

i. How many bits in the file `file2.txt`? [1 mark]

ii. How many attempts, on average, needed to perform a brute force attack on the ciphertext? [1 mark]

iii. What mode of operation was used? [1 mark]

(e) What is the name of the concept that aims to reduce the statistical nature of input plaintext in the output ciphertext of a block cipher? [1 mark]

(f) Explain an advantage of steganography compared to encryption. [1 mark]

(g) Explain a disadvantage of a 64-bit ideal block cipher. [1 mark]

(h) Consider a One Time Pad that uses hexadecimal (base-16) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of 10^9 messages per second. In theory, what is the average time to apply a brute force attack on this One Time Pad when a message is 200 characters? [1.5 marks]

(i) Explain one approach you can use to test if a cipher exhibits the avalanche effect. In your explanation make it clear what results you expect to see if the cipher exhibits the avalanche effect. [1.5 marks]

Question 5 [5 marks]

(a) Two security services are *confidentiality* and *authentication*. List and describe two other security services. [2 marks]

(b) Describe the difference between a *passive* and *active* attack on security. [1 mark]

(c) Describe two types of passive attacks. [2 marks]

Question 6 [4 marks]

(a) Decrypt the ciphertext *QDESWYARPEZY* with keyword *secretpassword* using the Playfair cipher. [4 marks]

Answer: _____

Question 7 [3 marks]

(a) If the output of `E/P` in the first round of S-DES is `10001101` and K_1 is `01101001`, then what is the output of `P4` in the first round? [3 marks]

Answer: _____

Question 8 [4 marks]

Calculate the following, showing calculations and assumptions. Answers without calculations will receive 0 marks.

(a) $\phi(24)$ [1 mark]

(b) Multiplicative inverse of 7 in (mod 15) [1 mark]

(c) 43267^{1873} mod 1961 [2 marks]

Question 9 [6 marks]

Consider a general Caesar cipher that uses the English lowercase letters, as well as two other characters—a space and a full stop. For mapping to numbers, the letters come first (i.e. $a = 0$), followed by space character and then finally the full stop (.) character. For example, the plaintext:

`This is an example.`

is valid as it uses only characters from the available set.

(a) Write an equation for decrypting ciphertext C to obtain plaintext P using this cipher. [1 mark]

(b) How many possible keys does this cipher have? [1 mark]

(c) The following ciphertext was obtained by encrypting plaintext P, a three word sentence, with the above cipher. What is the key and plaintext? [4 marks]

`brsaisaipcxj`

Plaintext: _____

Key: _____

Reference Material

S-DES operations

```
P8: 6 3 7 4 8 5 10 9  P10: 3 5 2 7 4 10 1 9 8 6
IP: 2 6 3 1 4 8 5 7  E/P: 4 1 2 3 2 3 4 1  P4: 2 4 3 1
```

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \quad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

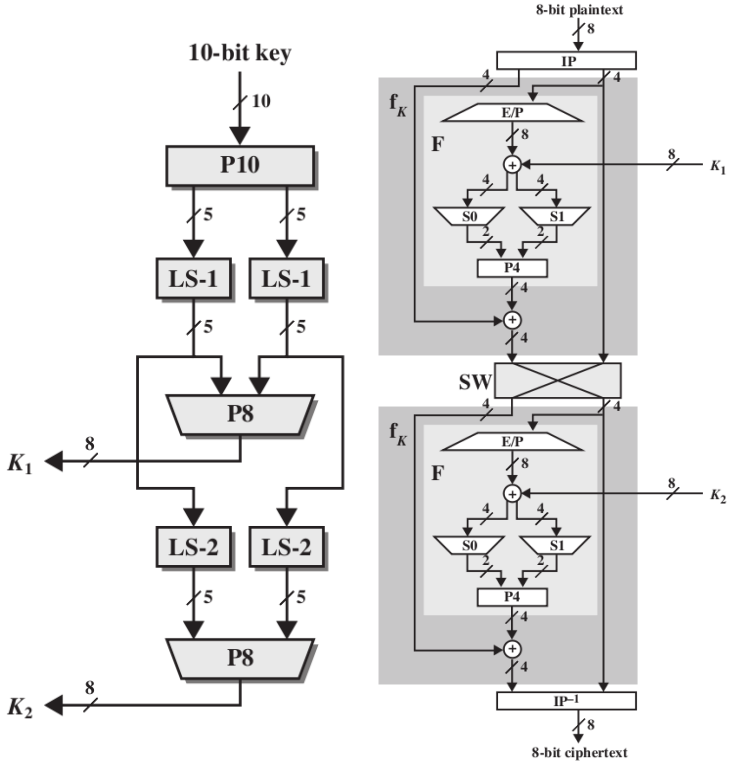


Figure 1: S-DES Key Generation and Encryption

Mapping of English characters to numbers

```
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
0 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
```

Fermat's theorem if p is prime and a is a positive integer, then $a^p \equiv a \pmod{p}$

Euler's theorem For positive integers a and n, $a^{\phi(n)+1} \equiv a \pmod{n}$

First 20 prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.

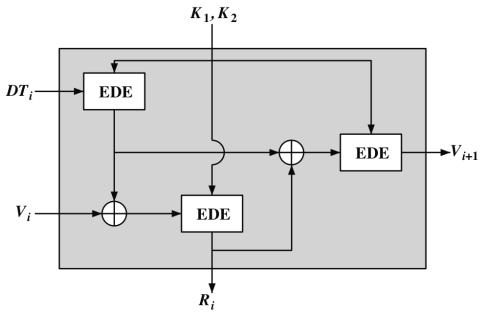
Linear Congruential Generator

$$X_{n+1} = (aX_n + c) \bmod m$$

Blum Blum Shub p, q are large prime numbers such that $p \equiv q \equiv 3 \pmod 4$; $n = p \times q$; s, random number relatively prime to n. Generate sequence of bits, B_i:

$$\begin{aligned} X_0 &= s^2 \bmod n \\ \text{for } i &= 1 \to \infty \\ X_i &= (X_{i-1})^2 \bmod n \\ B_i &= X_i \bmod 2 \end{aligned}$$

ANSI X9.17 See figure below:



Modes of operation

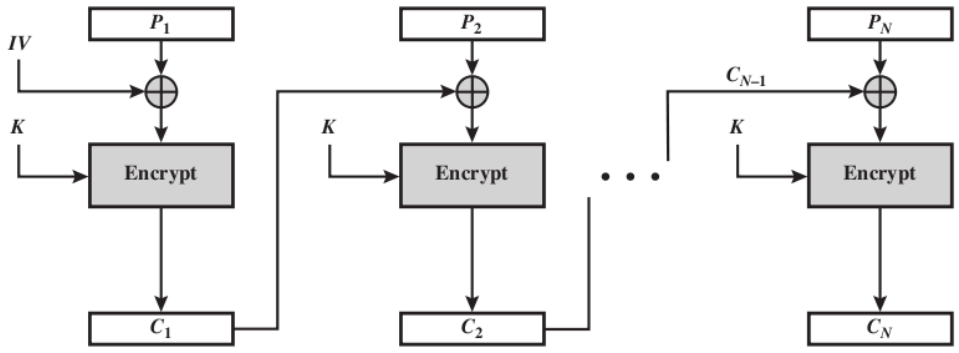


Figure 2: CBC mode of operation

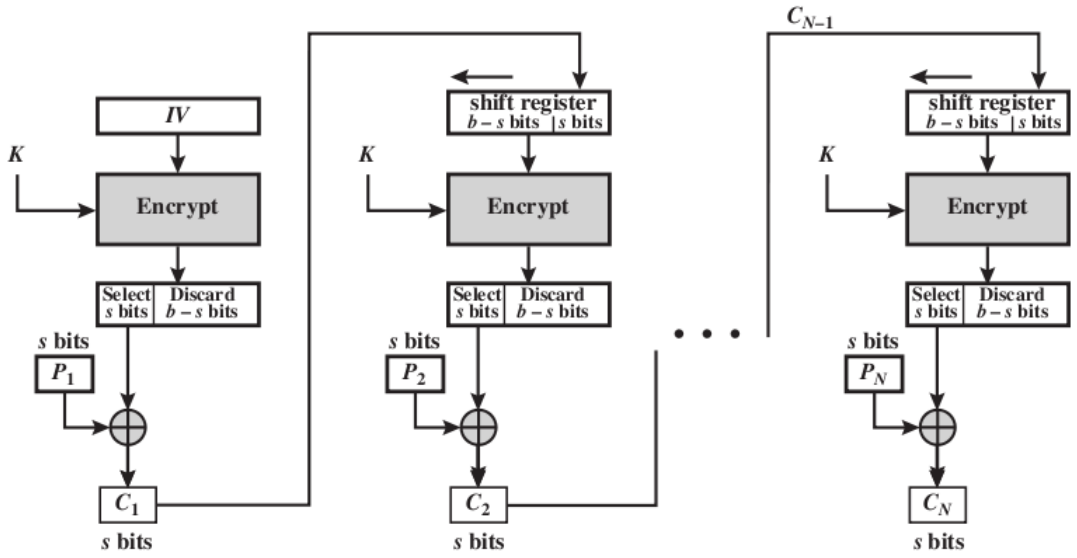


Figure 3: CFB mode of operation

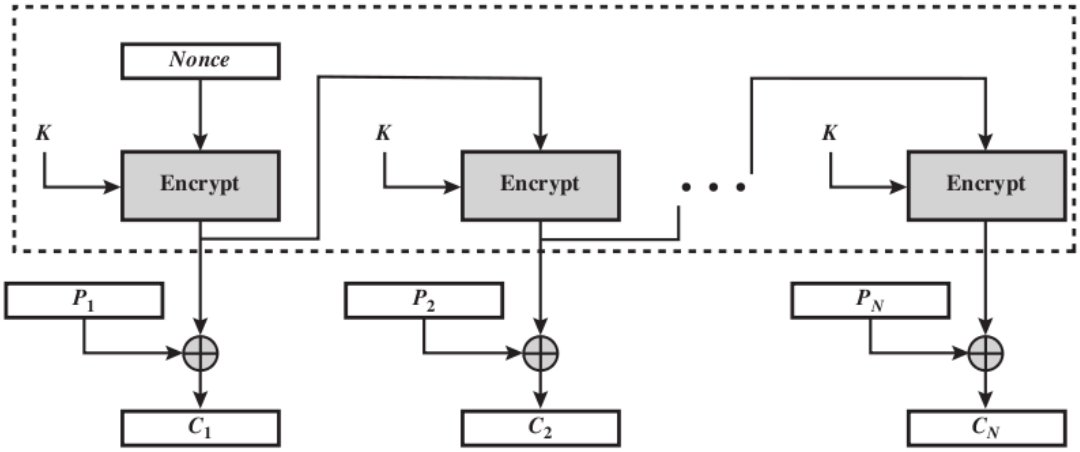


Figure 4: OFB mode of operation

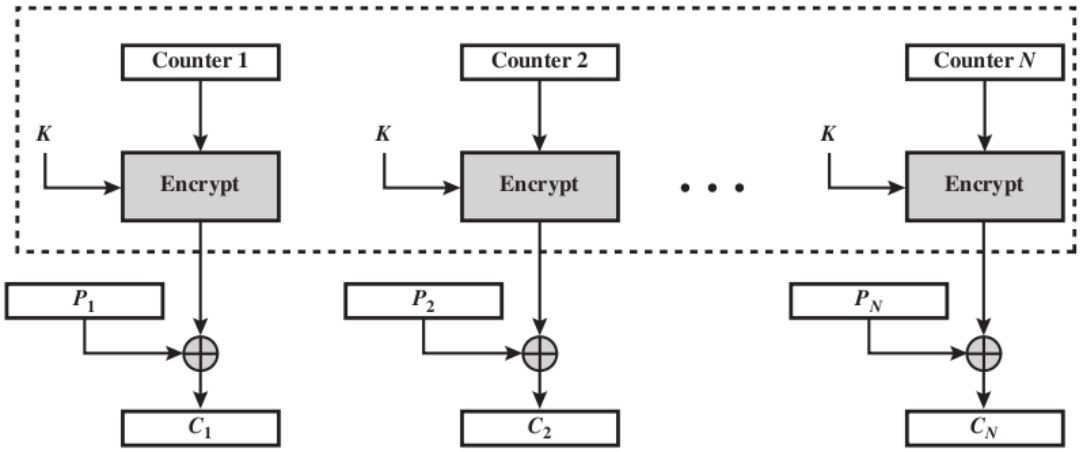


Figure 5: CTR mode of operation