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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2013

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Thursday 9 January 2014; 13:30–16:30

Instructions:

- This examination paper has 18 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.
- Turn off all communication devices (mobile phone etc.) and leave them at the front of the examination room.
- The examination paper is not allowed to be taken out of the examination room. A violation may result in score deduction.
- 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).
- Reference material included at the end of the exam may be used.

Question 1 [13 marks]

You have an RSA key pair of ($PU = \{7, 527\}, PR = \{343, 527\}$). You also know Steve and Thanaruk's public keys:

- Steve: $\{3, 319\}$
- Thanaruk: $\{7, 589\}$

You have a message, $M = 10$, to send confidentially to Steve.

(a) What is the value of the ciphertext that you send to Steve? [3 marks]

Answer: _____

(b) Note that you and Thanaruk have an identical e in your public key. In a real system, is it less secure if two users have the same value of e? Explain your answer. [1 mark]

Steve sent Thanaruk a confidential message. You intercepted the ciphertext, $C = 71$.

(c) What was the original plaintext, M? If an exponential is too large to perform accurately with your calculator then you may give your answer as an expression. For example, if your answer required calculating 12^{48} then you could write 12^{48} as the answer rather than trying to calculate it. Note 12^{48} is not the answer—its just an example of a value too large for your calculator. [6 marks]

Answer: _____

(d) Secure applications of RSA use much larger values than in the previous example. If sufficiently large values are used, then what are the three problems, all considered computationally infeasible, that an attacker must solve to break RSA? [3 marks]

Question 2 [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 can convince the target to decrypt ciphertext values that the attack has chosen, 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 "stevengordonstevengordonstevengo" > file1.txt
```

```
$ openssl enc -aes-128-cfb -in file1.txt -out file2.txt -nopad
-K f27036fbb28e554d -iv fd8a418a301fdca8
```

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

(f) 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^{10} messages per second. In theory, what is the worst case time to apply a brute force attack on this One Time Pad when a message is 300 characters? [1.5 marks]

(g) 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]

(h) If you wanted to compare two encryption algorithms, A and B, with respect to the randomness of the output they produce, explain two simple tests that can be performed. [2 marks]

Question 3 [9 marks]

(a) Encrypt the plaintext *hollow* using the Playfair cipher and keyword *steve* using the letter x as special padding if necessary. What is the ciphertext? [3 marks]

C = _____

The ciphertext *laizbsfavwwtwt* was obtained by encrypting using the Vigenère cipher with keyword *steve*. What was the plaintext? [3 marks]

P = _____

(b) The ciphertext *dselcetistshstuhetrrafeue* was obtained by encrypting using a rail fence cipher with key *5*. What was the plaintext? [3 marks]

P = _____

Question 4 [9 marks]

Consider a 4-bit block cipher, called *Steve's Simple Cipher* or SSC for short, shown in the table below. The table gives the ciphertext C produced when encrypting the plaintext P with one of the four keys.

P	C (K=00)	C (K=01)	C (K=10)	C (K=11)
0000	0110	1100	0001	0010
0001	1101	0100	1010	0000
0010	0010	0001	1111	1011
0011	0100	1101	0011	1001
0100	1100	0111	1001	0011
0101	1111	0101	0010	1000
0110	0000	0011	0111	1111
0111	0111	1011	1101	0001
1000	1010	1001	1000	0100
1001	0001	0000	1110	0111
1010	1001	0110	0110	1100
1011	1110	0010	1011	1101
1100	1011	1111	0000	0101
1101	1000	1010	0100	1110
1110	0011	1110	1100	0110
1111	0101	1000	0101	1010

(a) SSC is *not* an ideal block cipher. If SSC was to be extended to an ideal 4-bit block cipher, how many possible keys would it have? [1.5 marks]

(b) If SSC was extended to be an ideal 4-bit block cipher, how long would each key be? [1.5 marks]

(c) Give a reason why ideal block ciphers are not suitable in practice. [1 mark]

Consider a block cipher, *Double-SSC*, which involves applying the block cipher SSC 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 2-bit key.

(d) Show how the meet-in-the-middle attack works by applying it against Double-SSC. Use the attack to find the key used if the attacker already knows the (plaintext, ciphertext) pairs: (1101, 1100) and (1001, 1101). Explain clearly the steps applied by the attacker and how the key is identified. Write your answer below, and show calculations on next page. [5 marks]

`Key = _____`

Question 5 [7 marks]

A generalisation of the Caesar cipher is known as the *Affine Caesar cipher*. For each plaintext letter p, the ciphertext letter C is:

$$C = \mathrm{E}([a, b], p) = (ap + b) \bmod 26$$

For the Affine Caesar cipher to have a one-to-one mapping, the multiplicative inverse of a, or $\mathrm{MI}(a)$, in mod 26 must exist.

(a) Explain what is meant by a *one-to-one mapping* for a cipher. [1 mark]

(b) For $b = 4$ and $a > 3$, what is a value of a for which the Affine Caesar cipher has a one-to-one mapping? [1 mark]

(c) For $b = 4$ and $a > 3$, what is a value of a for which the Affine Caesar cipher does *not* have a one-to-one mapping? [1 mark]

(d) Using the syntax $\mathrm{MI}(a)$ for the multiplicative inverse of a, write an equation for the decryption operation of the Affine Caesar cipher. [2 marks]

(e) Assume the Affine Caesar cipher is extended for an n-character alphabet, i.e. instead of mod 26 it is mod n. Write an expression that gives the number of values of a for which a one-to-one mapping exists. Explain your reasoning, i.e. why the expression is valid. [2 marks]

Question 6 [7 marks]

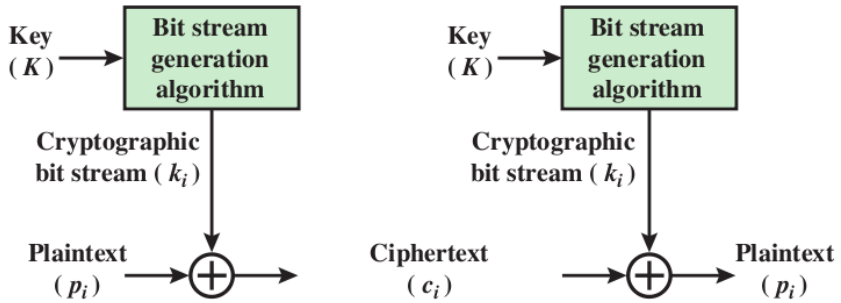
(a) List the name of four security services desired in computer networks. For each service, explain what the service means. [4 marks]

(b) Give the name of, and describe one active attack that can occur in computer networks. [1.5 marks]

(c) Give the name of, and describe one passive attack that can occur in computer networks. [1.5 marks]

Question 7 [7 marks]

The structure of stream ciphers is shown in the following figure. The bit stream generation algorithm is a PRNG.



(a) A problem with stream ciphers is that if key K is re-used with two different plaintexts p_1 and p_2, it is relatively easy for an attacker, once they find $p_1 \oplus p_2$, to determine the original plaintext values p_1 and p_2. Explain how an attacker can find $p_1 \oplus p_2$. [3 marks]

(b) To avoid the above problem, an initialisation vector (IV) is used with a secret to create input key K. That is, a secret key shared by the users S is chosen and combined with IV such that $K = S||IV$. While S remains the same for each plaintext encrypted, IV is incremented by 1. Explain how this avoids the above problem. [2 marks]

(c) If the secret S is 100 bits in length, and IV is 20 bits in length, then explain the condition in which the attacker could still find the plaintext using the approach in part (a). [2 marks]

Question 8 [6 marks]

The following ciphertext C was obtained by encrypting the original plaintext P with a Rows/Column Transposition cipher using a 5 digit key K_1, followed by encrypting the output of the Rows/Columns with a general Caesar cipher with key K_2. You can assume the most frequency letter in the plaintext P is 'e'. You also know the first word in the plaintext is four letters long. What is the original plaintext P?

```
C = lhszlplyueshadlletip

P = ________________________________________________
```

(Write your answer above; perform calculations below)

(space for answers)

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
```

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

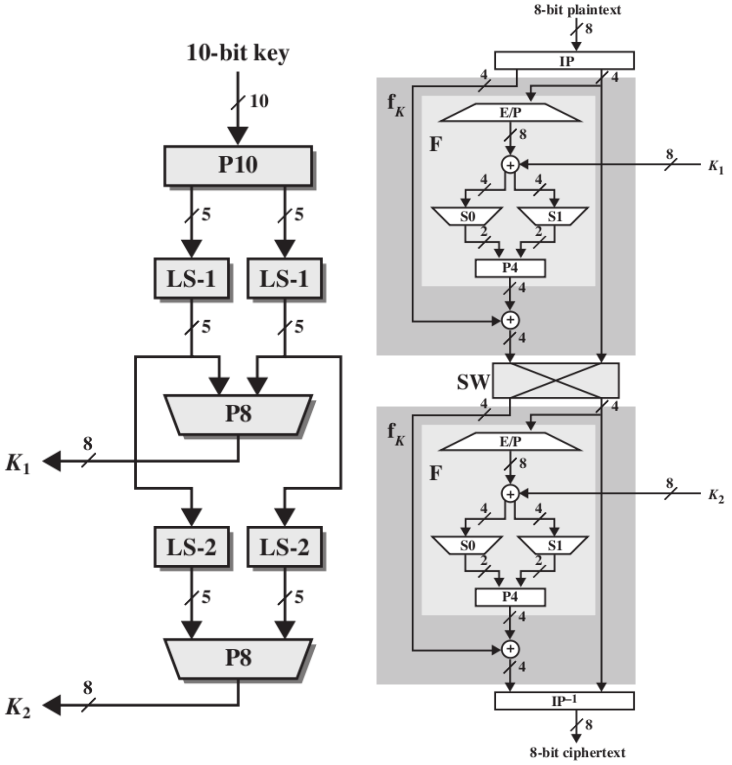


Figure 1: S-DES Key Generation and Encryption

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.

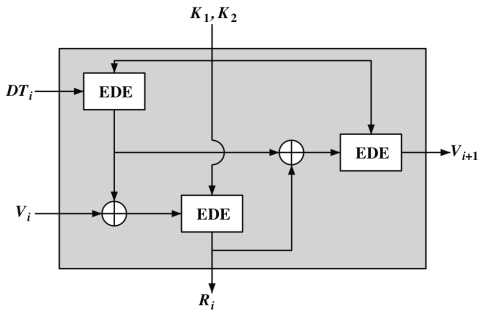
Linear Congruential Generator

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

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

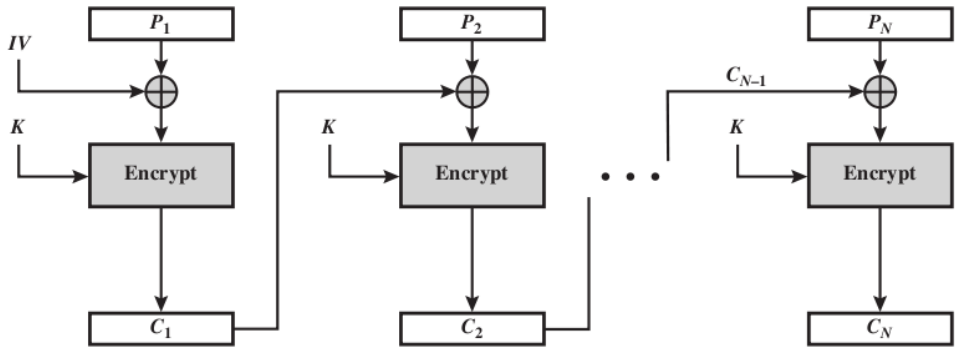


Figure 2: CBC mode of operation

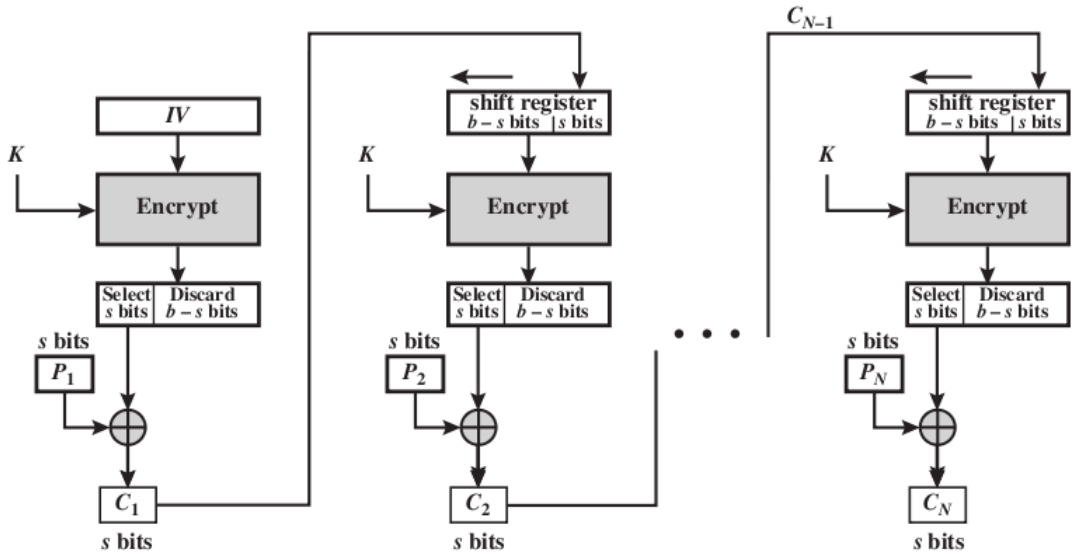


Figure 3: CFB mode of operation

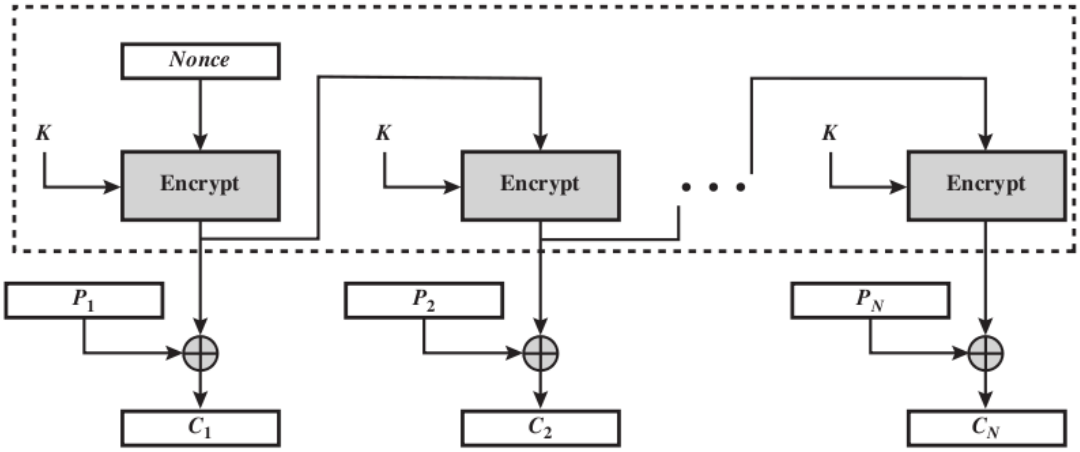


Figure 4: OFB mode of operation

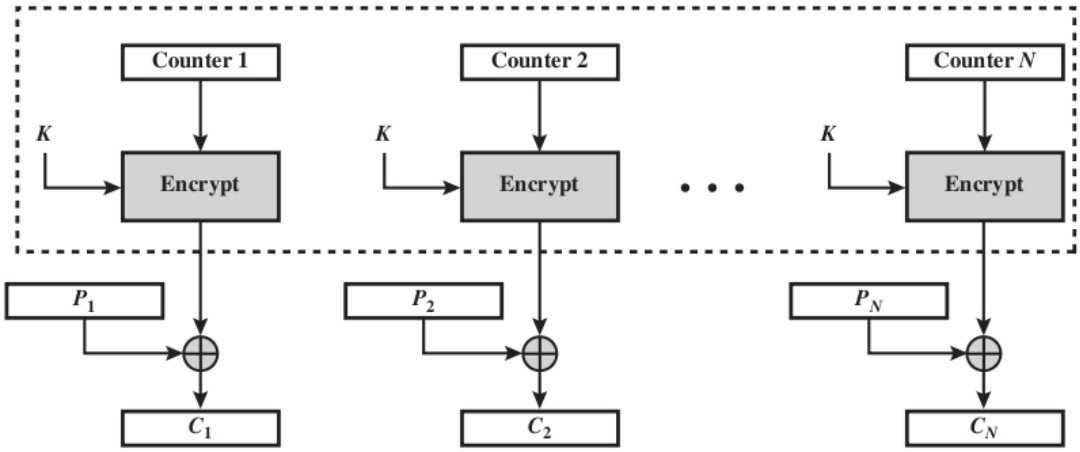


Figure 5: CTR mode of operation