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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2014

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Monday 2 March 2015; 13:30–16:30

Instructions:

- This examination paper has 20 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 [12 marks]

For each question fill in the blank space with an appropriate word, acronym, name or phrase. For each blank space you must give only one answer. However, there may be more than one correct answer. Each question is worth 1 mark.

(a) DES (and its variants, such as 3DES) is one example symmetric, block cipher. Another is _____.

(b) _____ is a security service that protects against a sender of a message denying that they ever sent that message.

(c) Any attack that alters the system resources is called _____ attack.

(d) A _____ attack involves a malicious user intercepting ciphertext and learning about communication patterns without obtaining the plaintext.

(e) A modification attack is an attack against the _____ service.

(f) A _____ attack includes the case of a malicious user sending many packets to a server to overload that server.

(g) A challenge with _____ key cryptography is the efficient and secure distribution of keys.

(h) Decryption with a stream cipher involves applying the _____ operation on the input stream of _____ and a keystream.

(i) The _____ is considered unconditionally secure.

(j) 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 _____.

(k) A brute force attack against a block cipher takes x seconds. A meet-in-the-middle attack against a double-version of the same block cipher would take approximately _____ seconds.

Question 2 [8 marks]

(a) Encrypt the plaintext *security* using the Playfair cipher and keyword *cryptography* using the letter x as special padding if necessary. What is the ciphertext? [4 marks]

C = _____

(b) The ciphertext *snosdunhoniisxanfofixncunfox* was obtained by encrypting using a rail fence cipher with key *4*. What was the plaintext? [4 marks]

P = _____

Question 3 [12 marks]

Consider an RSA public key $PU = \{11, 203\}$.

(a) Encrypt the message $M = 2$ using the public key. [2 marks]

C = _____

(b) Find the corresponding RSA private key. [4 marks]

PR = _____ , _____

(c) Consider the approach you used to find the RSA private key above. Assume instead of the small values used in this question, that large values are used (as recommended in practice). Explain two reasons an attacker would not be able to find the private key. [3 marks]

(d) Assume the attacker does not have the private key (and has no way to find it), explain two approaches that the attacker could try to find M if they intercepted C. Also explain why these two approaches are not realistic when using the recommended (large) values. [3 marks]

Question 4 [10 marks]

(a) If the "avalanche effect" is present in a cipher, is that an indicator of a strong cipher or a weak cipher? [1 mark]

(b) Explain one method to test for the avalanche effect in a cipher. [2 marks]

(c) On average, how many days would it take a computer that can decrypt at a speed of 10^{12} operations per second to be successful in a brute force attack on a 64-bit key? [2 marks]

(d) If the cipher that is being attacked in part (c) is using CBC mode of operation, can the attack duration be shortened by using multiple computers at the same time? Explain your answer. [2 marks]

(e) Attacks on ciphers are usually measured in terms of: time, memory and known data. For each of these three metrics, compare a brute force attack on DES with a MITM attack on Double-DES, indicating approximately how much time/memory/known data is needed for one attack (relative to the other attack). [3 marks]

Question 5 [10 marks]

Consider a block cipher, *ABC*, which 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) Assuming CBC was used with *ABC*, decrypt the ciphertext `11110110` using the key `001` and initialisation vector `1110`. Show your calculations in the space below, and write your final answer on the line below. [3 marks]

Plaintext: _____

(b) Consider the cipher ABC being used in Counter Mode to act as a pseudorandom number generator. If the initial value of the counter is 0000 and the seed is 101, then what are the first 12 pseudorandom bits? [3 marks]

Bits: _____

(c) What is the maximum period, in bits, of the above PRNG? [2 marks]

(d) Different tests can be used to check if a sequence of bits does not appear random. One such test is to count the number of 0's and 1's in the entire sequence: if there are not approximately equal number of 0's and 1's then the sequence does not appear to be random. Describe two other tests. [2 marks]

Question 6 [7 marks]

The table below shows the ASCII table. Note that each character maps to a 7-bit value.

Last 4 bits \ First 3 bits	000	001	010	011	100	101	110	111
0000	NUL	DLE	SP	0	@	P	‘	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EOT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	’	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	’	<	L	\	l	|
1101	CR	GS	–	=	M	]	m	}
1110	SO	RS	·	>	N	^	n	~
1111	SI	US	/	?	O	–	o	DEL

Figure 1: ASCII Table

(a) If a binary one-time pad is used with key `10110001100010110001O` to obtain the ciphertext `kPP`, then what is the plaintext (in ASCII characters, not binary)? Show or explain your steps. (Hint: you should recognise the plaintext) [3 marks]

Answer: _____

(b) In general, the OTP has two requirements on the key that the Vigenere cipher does not. What are the two requirements? [2 marks]

(c) Explain a problem with the key in part (a). [2 marks]

Question 7 [9 marks]

(a) If the input of `E/P` in the first round of S-DES is `1101` and K_1 is `01011000`, then what is the input of `P4` in the first round? [3 marks]

Answer: _____

(b) If the input of the 2nd round of S-DES is `10010110`, and the output of `P4` in the 2nd round is `1011`, then what is the ciphertext? (Note: the input of the 2nd round is the same as the output of the SWap operation). [3 marks]

Answer: _____

(c) If you know the ciphertext as well as the input of the 2nd round of S-DES, then which step(s) make it difficult to find K_2? Explain your answer. [3 marks]

Question 8 [6 marks]

Consider a public-key crytposystem with three users: A, B, and C. Assume all necessary keys have been created and distributed to the relevant users.

(a) List the set of keys that user A knows (or can easily discover). [1 mark]

(b) List the set of keys that user A knows, but users B and C do not. [1 mark]

(c) If user A wants to send a confidential message M to user B, then explain what user A does. [1 mark]

(d) Explain why the message M is confidential, i.e. user C cannot read it. [1 mark]

(e) If user C wants to send an authenticated message M to user B, then explain what user C does. [1 mark]

(f) Explain how C is certain the message comes from B, and not A pretending to be B. [1 mark]

Question 9 [6 marks]

Note: this question may take a large amount of time if you don't follow a good approach. It is only worth 6 marks. Therefore I suggest attempting it only after you have attempted all other questions.

A plaintext message was encrypted using a rows/columns transposition cipher (using a key length of less than 10 characters), followed by a Caesar cipher, to produce the ciphertext:

```
zbtkxhnabgtxbbggfzbmfmmm
```

You've discovered that no padding was used (or was necessary) in any of the ciphers. You also know the most frequent character in the plaintext is *i*, the first letter in the plaintext is *t*, the first word in the plaintext is 6 characters long, and the plaintext contains the word *the*. What is the full plaintext message?

Answer: _____

(continue answer if necessary)

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
```

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

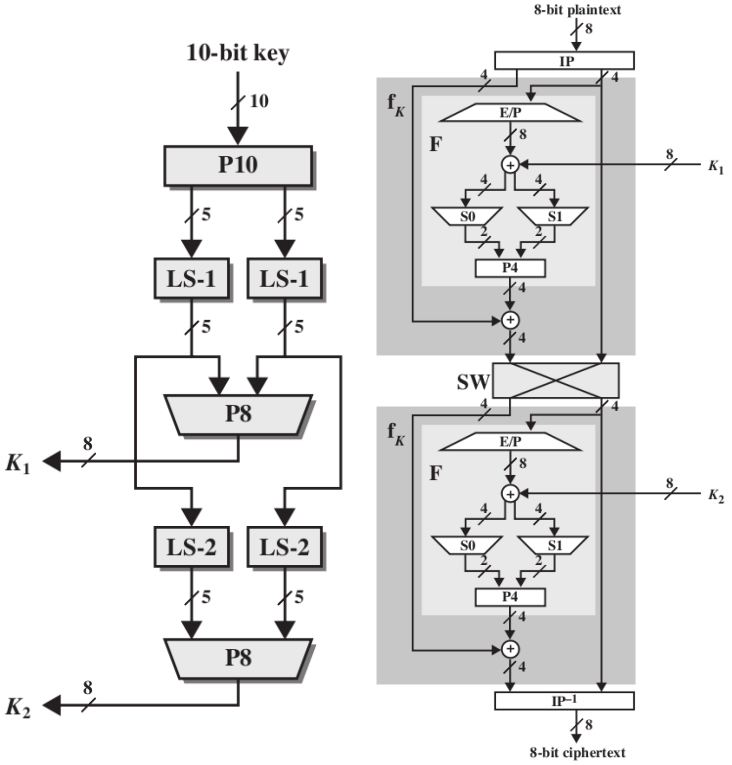


Figure 2: S-DES Key Generation and Encryption

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.

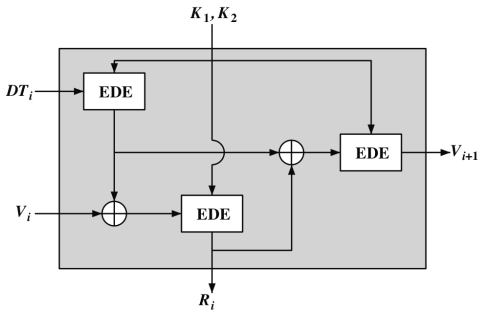
Linear Congruential Generator

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

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

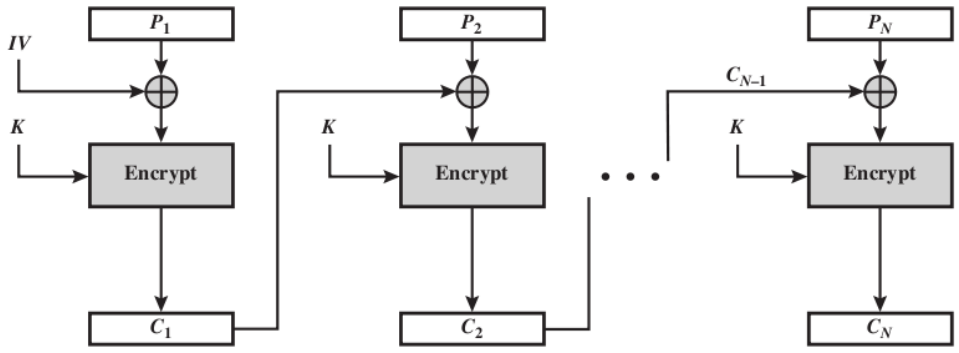


Figure 3: CBC mode of operation

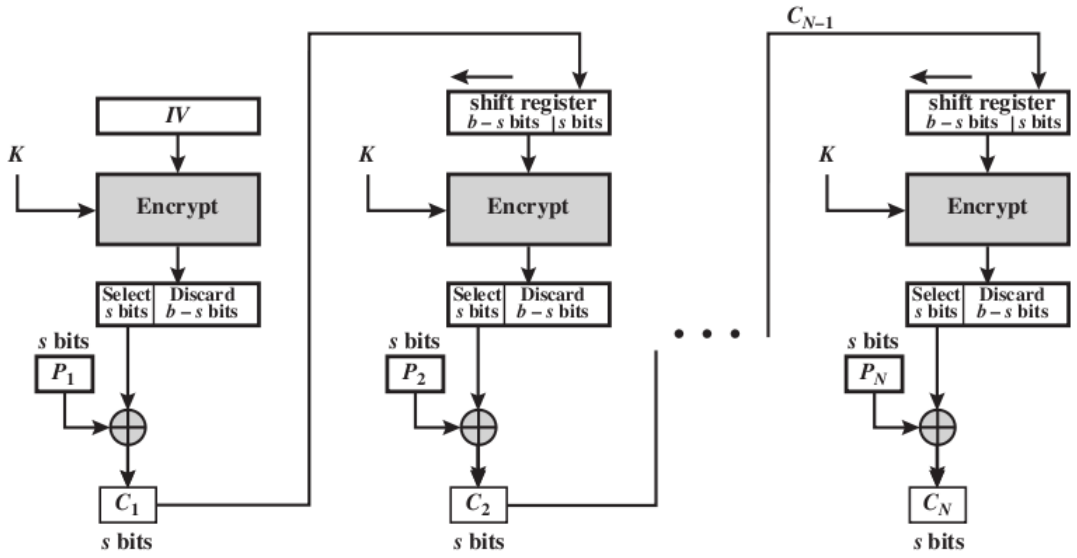


Figure 4: CFB mode of operation

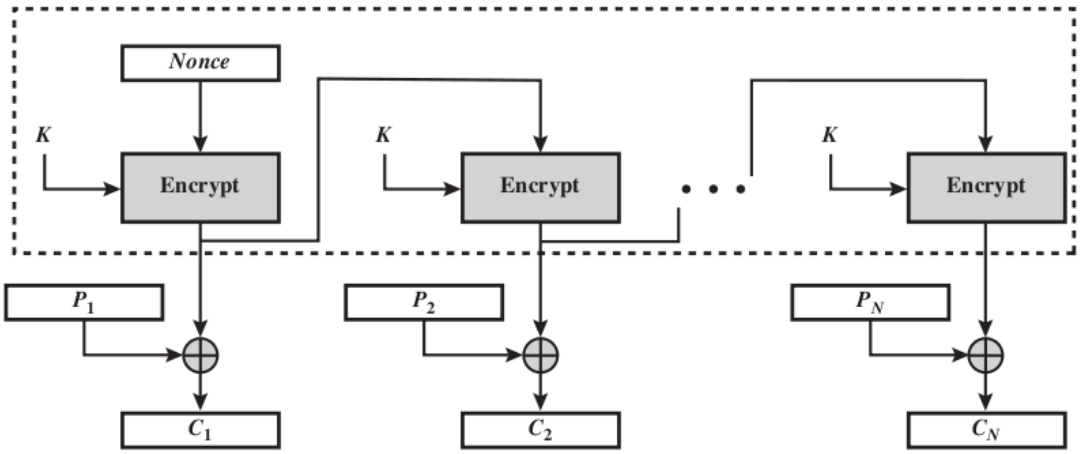


Figure 5: OFB mode of operation

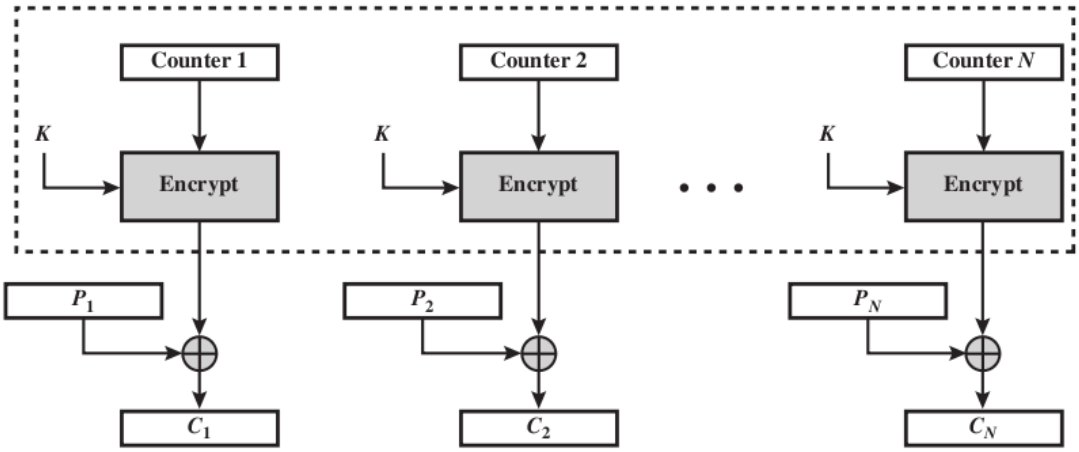


Figure 6: CTR mode of operation