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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2011

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Tuesday 21 February 2012; 9:00–12:00

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.
- 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 [30 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 answer is worth 1.5 marks.

(a) _____ is a standalone command line program, as well as a library of functions that can be called by other programs, that provides common cryptographic operations symmetric and asymmetric ciphers.

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

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

(d) If a cryptanalyst knows only the encryption algorithm being used, ciphertext, and ciphertext chosen by the cryptanalyst together with its corresponding decrypted plaintext, then an attack can be classified as _____.

(e) Consider the basic terminology used in models of ciphers. The process of converting a coded message back to the original message is called _____.

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

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

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

(i) _____ was used in the homework to encode binary ciphertext into a format that can be sent in the contents of plaintext emails.

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

(k) In public key cryptography, to provide authentication user A sends a message to user B encrypting using the _____ key of user _____.

(l) The _____ is considered unconditionally secure.

(m) Confusion can be achieved using a non-linear substitution algorithm. In DES such a substitution is performed using _____.

(n) In S-DES the initial permutation is defined as [2 6 3 1 4 8 5 7]. Therefore IP^{-1} is defined as _____.

(o) 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.

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

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

(r) The _____ for block ciphers was developed to overcome practical problems of an ideal block cipher.

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

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

Question 2 [13 marks]

You have an RSA key pair of ($PU = \{19, 323\}, PR = \{91, 323\}$). You also know Steve and Thanaruk's public keys:

- Steve: $\{61, 437\}$
- Thanaruk: $\{13, 253\}$

Thanaruk sent Steve a confidential message. You intercepted the ciphertext, $C = 3$.

(a) What was the original plaintext, M? [10 marks]

Answer: _____

(b) 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 3 [4 marks]

(a) Consider the Linear Congruential Generator as a PRNG. For the values of $a = 3$, $c = 1$, $m = 63$ and a seed of 12, what are the next 3 numbers in the pseudo-random sequence? [3 marks]

Answer: _____

(b) Which of the parameters of the above LCG should be changed to produce a sequence with a larger period? What is a suggested value? [1 mark]

Question 4 [7 marks]

You are using Diffie-Hellman to exchange a secret, K, with Steve. You've already agreed on public values $\alpha = 3$ and $q = 19$. You have chosen $X_{you} = 10$. Steve has sent you $Y_{Steve} = 2$.

(a) What is the value of the secret, K? [3 marks]

Answer: _____

(b) What is the value of Steve's private number, X_{Steve}? [4 marks]

Answer: _____

Question 5 [14 marks]

You have a plaintext message in an 8KB file to be encrypted using Triple-DES. Your computer has a quad-core CPU. Although modes of operation can utilise all cores when possible, your implementation of single (normal) DES uses just one core at a time. Benchmarks have shown that a single core of your CPU can perform DES encryptions at a speed of 100,000 per second (decryptions are the same speed as encryption; other operations that may be needed in different modes of operation, like XOR, or very fast, effectively taking zero time).

(a) How long does it take your computer to encrypt the entire plaintext if using CBC? [3 marks]

Answer: _____

(b) How long does it take your computer to encrypt the entire plaintext if using CTR? [3 marks]

Answer: _____

You select a mode of operation, encrypt the plaintext and send the ciphertext across a network. However there is one bit in error in the received ciphertext at the destination: the 644th bit transmitted was a 0, but the bit is received as a 1. The destination doesn't know of the bit error, i.e. no error detection, and decrypts the received ciphertext.

(c) If the mode of operation you chose was CBC, how much of the received plaintext would be correct? Give your answer in number of blocks or Bytes. Explain your answer. [3 marks]

Answer: _____

(d) If the mode of operation you chose was OFB, how much of the received plaintext would be correct? Give your answer in number of blocks or Bytes. Explain your answer. [3 marks]

Answer: _____

Assume now that there were no bit errors in the data transmission (the ciphertext received by the destination is identical to that originally sent). CBC takes an initialisation vector (IV) as input, whereas OFB takes a Nonce as input. Assume you have many files to encrypt using Triple-DES over a long period and you want to use the same key.

(e) Explain why it is sufficient to use the same IV for CBC for each file, but for OFB it is better for security if a different Nonce is used for each file. [2 marks]

Question 6 [8 marks]

(a) Encrypt the plaintext *shannon* with keyword *genius* using the Playfair cipher. [4 marks]

Answer: _____

(b) Decrypt the ciphertext *isrevhnmsmdnrtileaaa* with the key *41253* using the Rows/Columns transposition cipher. [4 marks]

Answer: _____

Question 7 [9 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. [3 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. [3 marks]

Question 8 [6 marks]

(a) If you wanted to compare two encryption algorithms, A and B, with respect to the avalanche effect, explain two methods in which they can be compared. [3 marks]

(b) 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. [3 marks]

Question 9 [9 marks]

A plaintext message was encrypted using a rail-fence transposition cipher, followed by a Vigenere cipher, to produce the ciphertext:

`kzikgwpxavgbenkmvxanmcgvlakg`

You've discovered that no padding was used (or was necessary) in the rail-fence and that the Vigenere keyword was 4 characters long. Also, given your knowledge of the topic, you've guessed (correctly) that the first word of the plaintext is *security*. 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
```

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

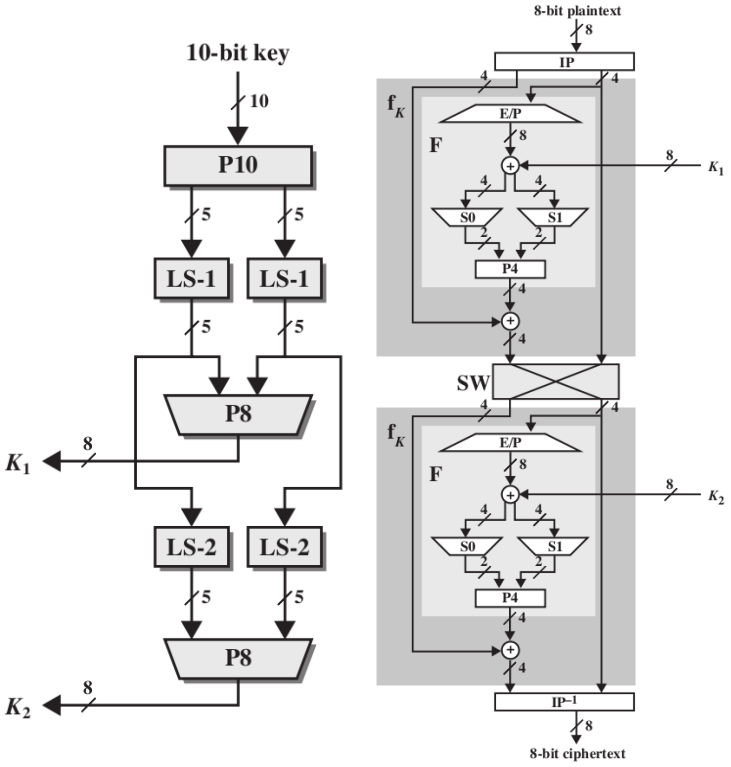


Figure 1: S-DES Key Generation and Encryption

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, $a^{\phi(n)+1} \equiv a \pmod{n}$

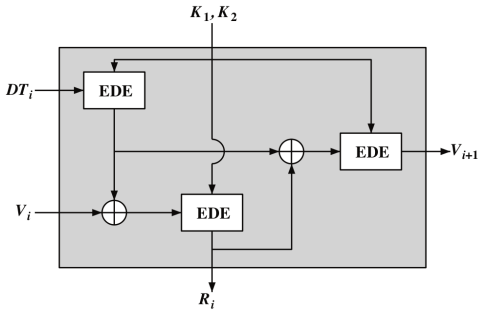
Linear Congruential Generator

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

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

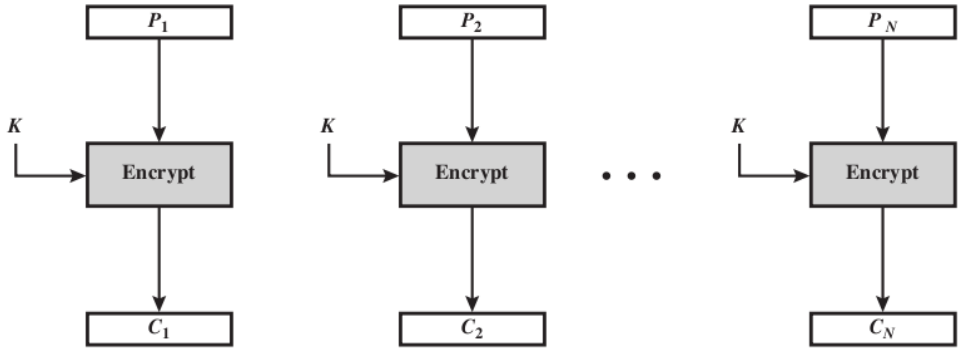


Figure 2: ECB mode of operation

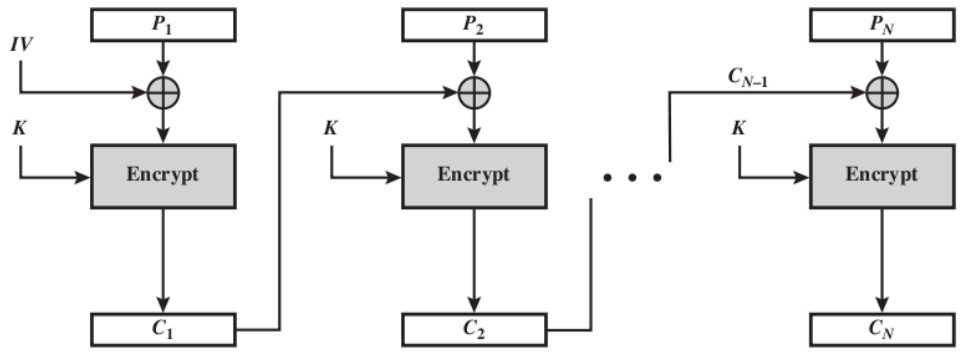


Figure 3: CBC mode of operation

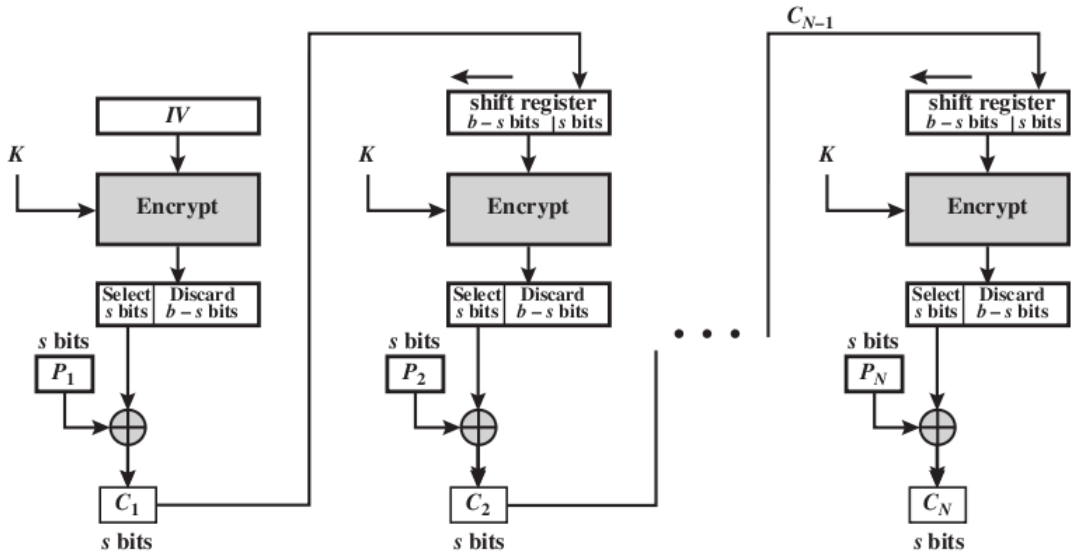


Figure 4: CFB mode of operation

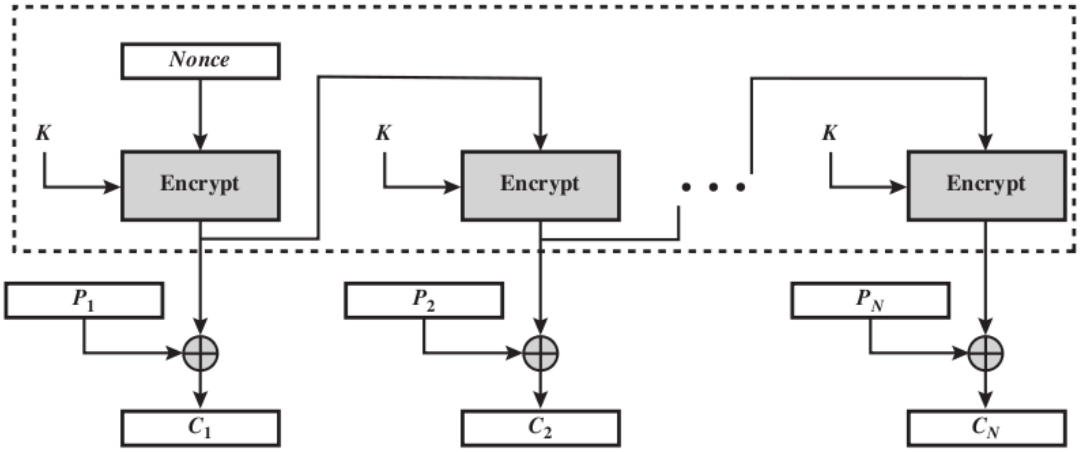


Figure 5: OFB mode of operation

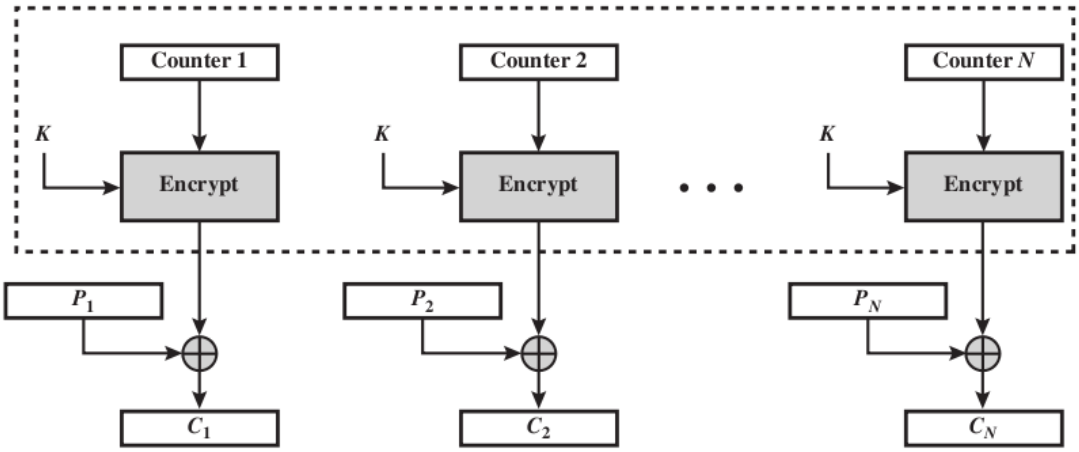


Figure 6: CTR mode of operation