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).

CSS322 Midterm Exam Hints 2011

- 9 questions, each with multiple parts
- Total of 100 marks
- Question 1 is a set of "fill in the blank" questions.
- Questions 2 to 9 are longer questions
- Some questions may take a long time to solve. Read through all questions at the start of the exam and allocate your time to maximise your marks.
- For questions that you consider will take a long time to solve, think carefully about your approach before starting your attempt (there may be multiple approaches, some much faster than others).
- In some questions there is a specific area to write your answer, e.g.:

  Answer: _____

  Use the space below it to show your calculations/explanations, and write your final answer on the line provided (this makes it easier for me to find your final answer).
- Show calculations/explanations where necessary – partial credit will often be given even if you arrive at the incorrect final answer.
- Use past exams and quizzes for study material.
- Topics covered: Introduction to Security through to Public Key Cryptography (inclusive)
- The following pages (Reference Material) are given at the end of the exam – you don't have to memorise it. Classical ciphers, RSA, Diffie-Hellman and other details not in the Reference Material are not provided in the exam. That is, you will need to remember them (if there is a question). You do not need to memorize all the steps of full DES, RC4, AES or similarly complex algorithms.

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
```

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

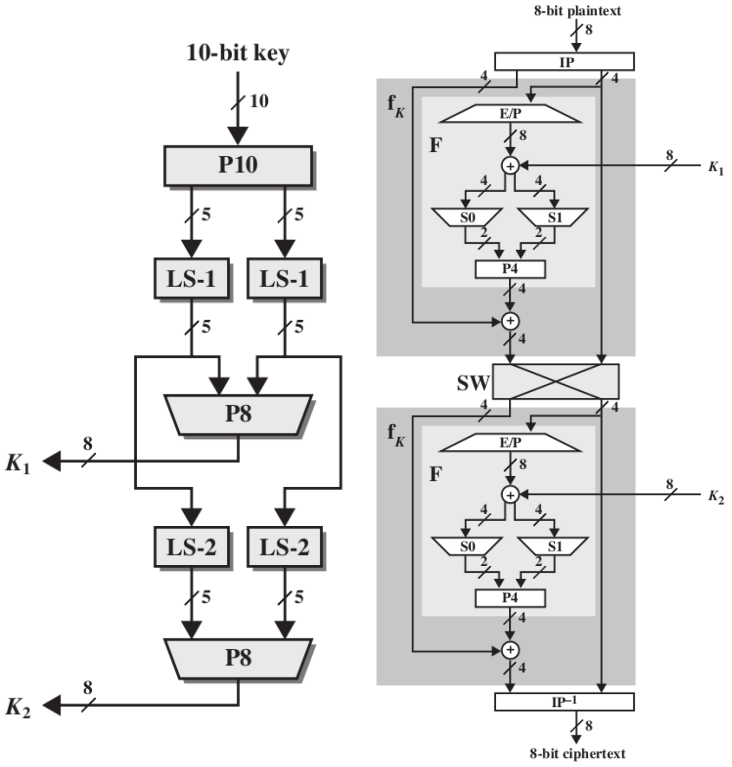


Figure 1: S-DES Key Generation and Encryption

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

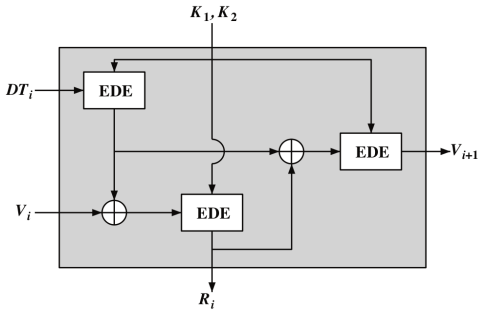
Linear Congruential Generator

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

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

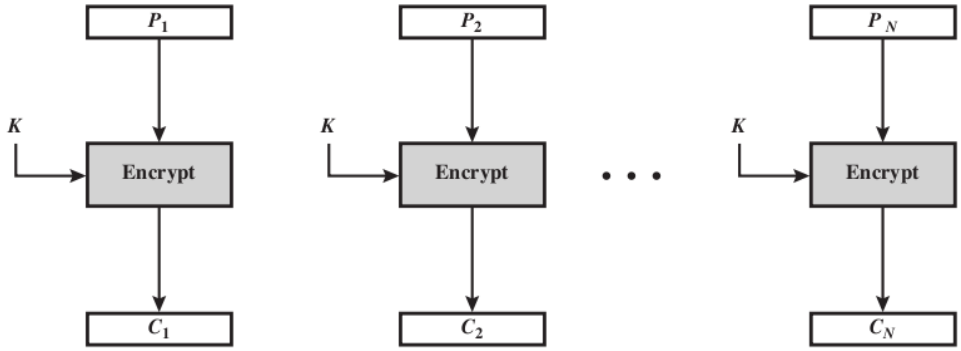


Figure 2: ECB mode of operation

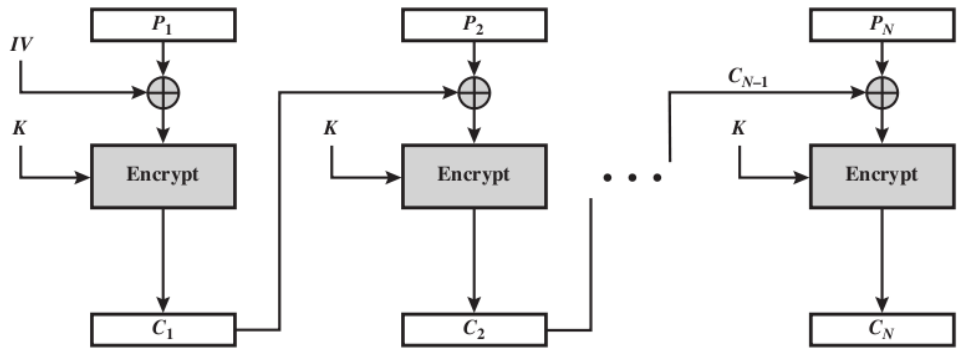


Figure 3: CBC mode of operation

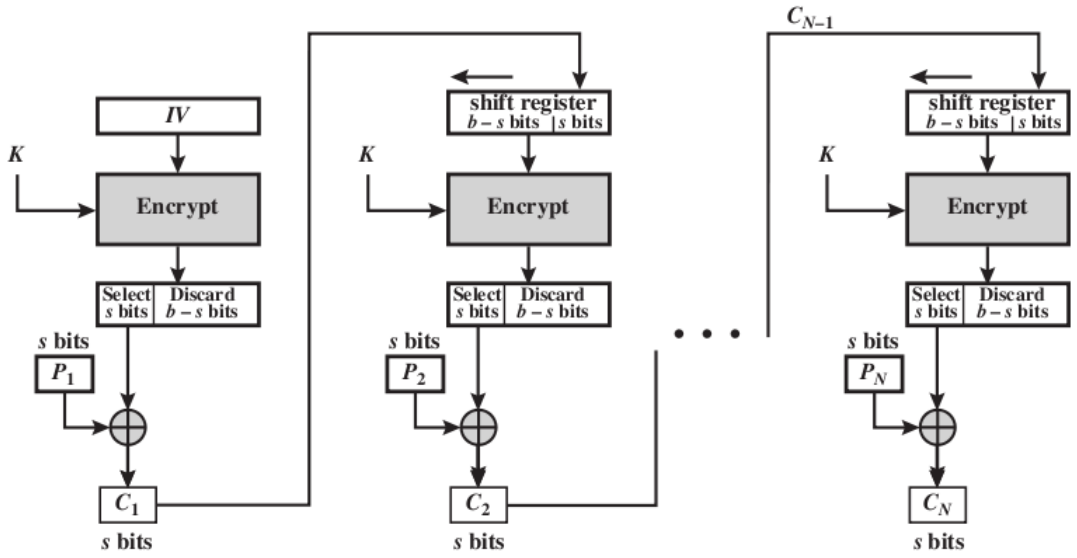


Figure 4: CFB mode of operation

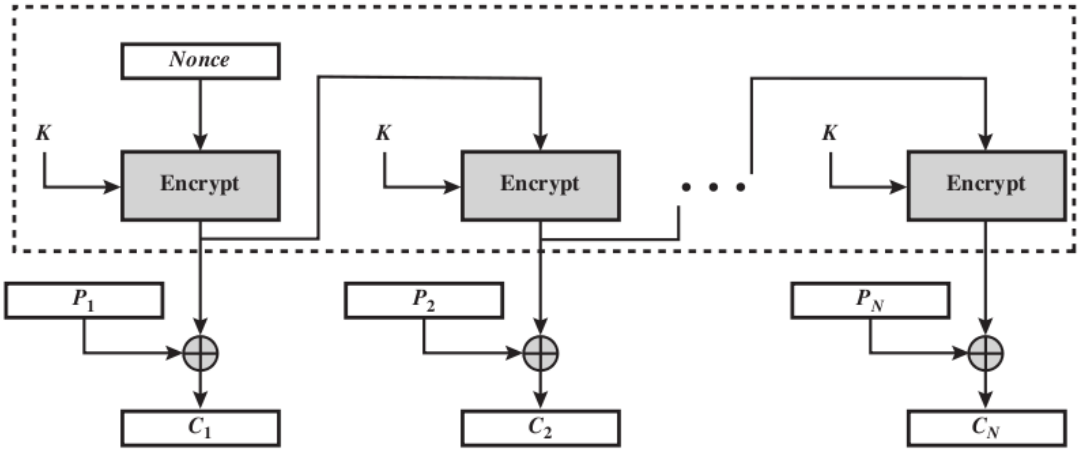


Figure 5: OFB mode of operation

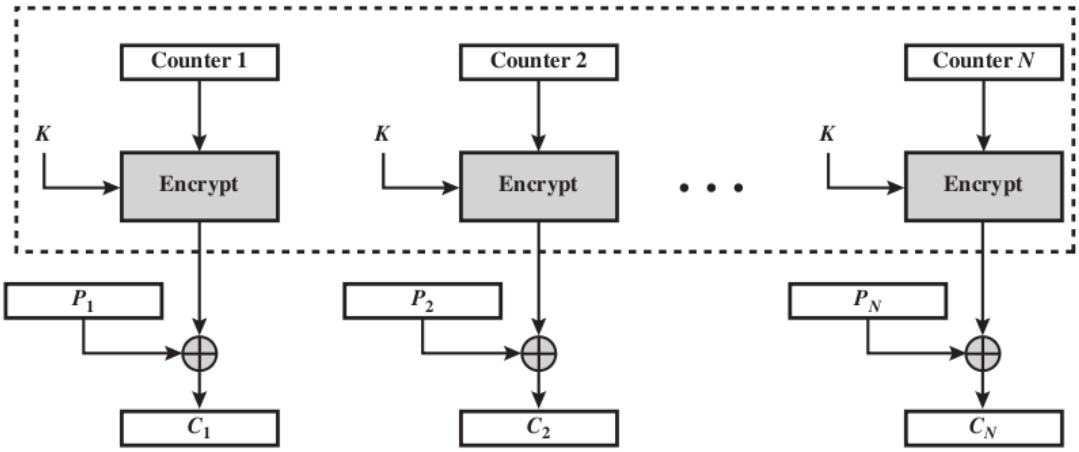


Figure 6: CTR mode of operation