

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.

Hints

- 8 questions, each with multiple parts
- 70 marks in total
- Covered topics:
 - Intro to security, e.g. services, attacks, mechanisms
 - Classical ciphers, including encrypting/decrypting with the classical ciphers covered in lectures, as well as concepts of ciphers
 - DES and block ciphers. You don't have to remember the details of DES/S-DES, but if the details are given, you may have to use/interpret them. See Reference Material for example.
 - Modes of operation: you don't have to remember how they will work but may need to use them (see Reference Material)
 - Stream and PNRG
 - Number Theory: you may need to use the theory we covered; see Reference material for equations that are given.
 - Public Key cipher: concepts and details of RSA. You may need to remember the details of RSA (it is not given in Reference Material).
- Past exams are excellent practice and examples of questions
- Quizzes and homeworks are good practice and examples of questions
- Calculator is allowed, but if you do not bring one then you can answer all questions. If a value is too large to calculate (in your head or even by calculator) then you can give an expression as an answer, e.g. 123^{456} .

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

$$S_0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \quad S_1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

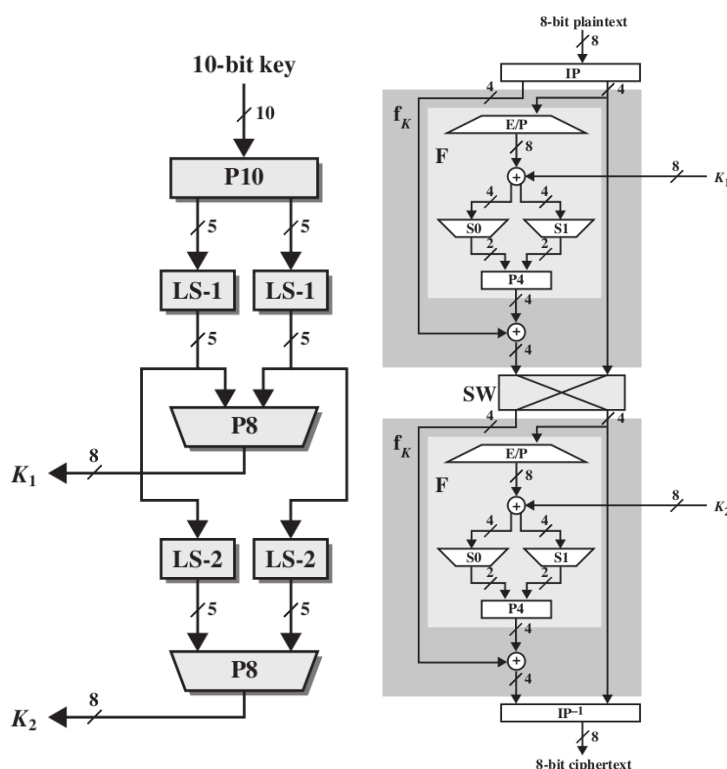


Figure 1: S-DES Key Generation and Encryption

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.

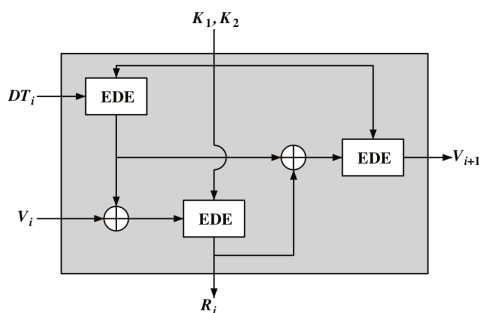
Linear Congruential Generator

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

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 :

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

ANSI X9.17 See figure below:



Modes of operation

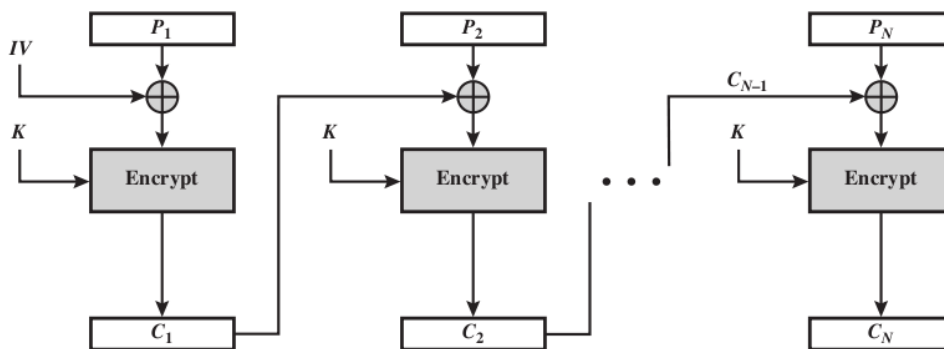


Figure 2: CBC mode of operation

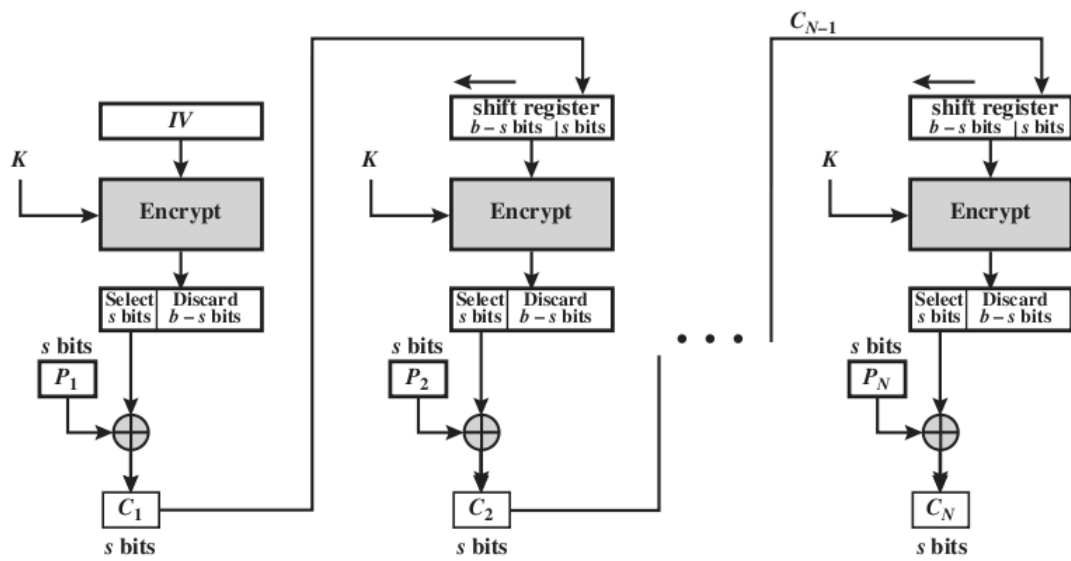


Figure 3: CFB mode of operation

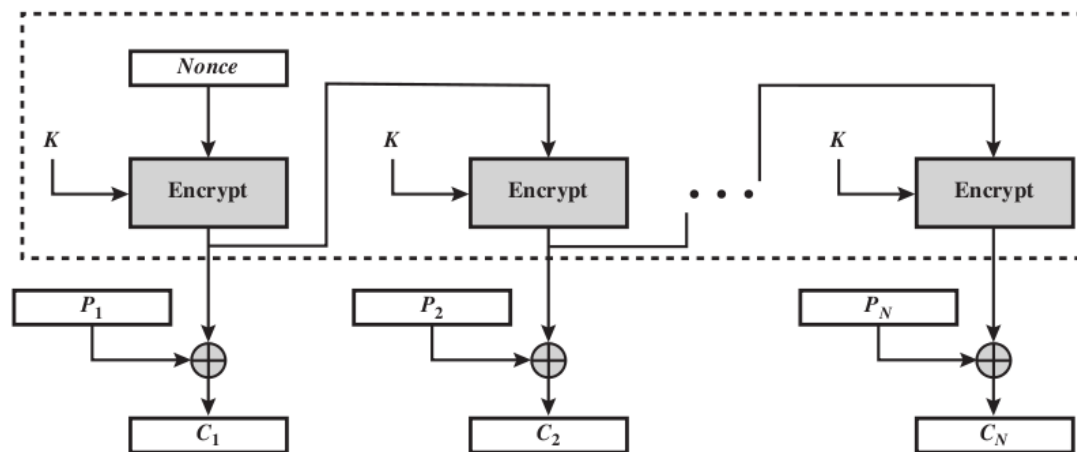


Figure 4: OFB mode of operation

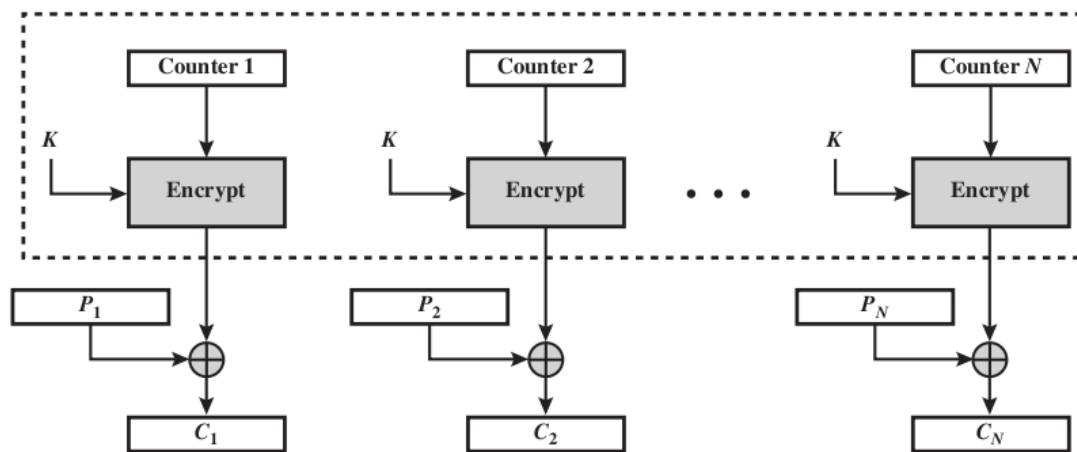


Figure 5: CTR mode of operation