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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam Answers: Semester 2, 2012

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Friday 21 December 2012; 13:30–16:30

Instructions:

- This examination paper has 16 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 [7 marks]

The original IEEE 802.11 wireless LAN protocol used Wired Equivalent Privacy (WEP) for data confidentiality. WEP requires a b-bit secret key, K, shared by sender and receiver (e.g. laptop and access point). For every packet containing n Bytes of data to be sent, WEP concatenates a 24-bit initialisation vector, IV, with the key K, and uses the resulting value as the input to the stream cipher RC4. A n Byte keystream, s, is generated by RC4, which is then used to encrypt the packet. For each new packet, RC4 is applied again, using the same K but different IV (it is incremented by 1 for each packet) to generate a new keystream. The keystream generation can be written as: $s = RC4(K||IV, n)$. The IV is not secret; it is sent, unencrypted, in the header of the corresponding packet.

The operation RC4(*input*, n) can be summarised as:

- Initialise state and temporary vectors based upon *input*
- Perform initial permutation on state vector
- Loop n times: in each loop permutate the state vector and generate a byte of the keystream.

(a) Write an equation for the WEP encryption. That is, given plaintext P (the packet data) as input, how is ciphertext C calculated? Use the variables/notation from the above description. Hint: your answer may include s. [1 mark]

Answer. *The ciphertext for a packet is obtained by XORing the plaintext with the keystream:*

$$C = P \oplus s$$

(b) Consider if WEP did not use an IV. Instead, for each packet, RC4 is applied using K as input and producing s as output. Assume RC4(K, n) is applied for each packet and that all packets are the same length. In this case, WEP would be considered very weak. This is because if an attacker can capture just two packets (containing ciphertext) and find a value which is equivalent to the XOR of two plaintexts, i.e. $P_1 \oplus P_2$, assuming the plaintexts are structured (e.g. English messages) then it is relatively easy to find the values of P_1 and P_2. Hence the challenge for the attacker is to find $P_1 \oplus P_2$. Explain how the attacker can find $P_1 \oplus P_2$. [3 marks]

Answer. *If the same key K is used as input the RC4, then the same keystream will be produced, s. So when encrypting packet 1, the ciphertext is $C_1 = P_1 \oplus s$. And when encrypting packet 2, the ciphertext is $C_2 = P_2 \oplus s$. The attacker knows the ciphertext values, C_1 and C_2. Now using the properties of XOR the attacker can do the following:*

$$\begin{aligned} C_1 \oplus C_2 &= (P_1 \oplus s) \oplus (P_2 \oplus s) && (1) \\ &= P_1 \oplus P_2 \oplus s \oplus s && (2) \end{aligned}$$

$$= P_1 \oplus P_2 \quad (3)$$
$$(4)$$

So now the attacker knows $P_1 \oplus P_2$, and in many cases it is easy to find P_1 and P_2.

(c) Explain how the use of a 24-bit IV makes the trivial attack from part (b) more difficult. Hint: consider how many packets need to be captured. [2 marks]

Answer. *Since a different IV is used for each packet, a different keystream will be used for each packet. That is, $C_1 = P_1 \oplus s_1$ and $C_1 = P_1 \oplus s_2$, where $s_1 \neq s_2$. So by capturing two packets, the attacker will not be able to find $P_1 \oplus P_2$. They need to capture many more packets. Since the IV is 24-bits long, it will repeated after 2^{24} packets. So if the attacker captures about 17 million packets, then they can find $P_1 \oplus P_2$, because for two of those packets $s_1 = s_2$.*

(d) WEP has other, related problems, which has meant a new protocol has been developed for wireless LANs called WiFi Protected Access (WPA). WPA uses AES instead of RC4. What is a disadvantage of using AES compared to RC4? [1 mark]

Answer. *AES, a block cipher, is more complex and generally a slower implementation than RC4.*

Question 2 [5 marks]

Consider a block cipher, *Double-ABC*, which involves applying the block cipher *ABC* 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 3-bit key. The cipher *ABC* 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) What is the plaintext when decrypting ciphertext `0011` using key `100111` using *Double-ABC*? [1 mark]

Answer. *1011*

(b) You, as an attacker, have discovered the following past plaintext-ciphertext pairs that two users generated using *Double-ABC* and some key K. Find the key using a meet-in-the-middle attack. [4 marks]

- $P_1 = 0110, C_1 = 0100$
- $P_2 = 1111, C_2 = 1101$

Key: _____

(space for calculating key is below; write your final answer on previous page)

Answer. *Considering the first pair, encrypt the plaintext with all possible values of K_1, and also decrypt the corresponding ciphertext with all possible values of K_2.*

$$P = 0110$$

$$K_{1,1} = 000 : X_{1,1} = 0010$$
$$K_{1,2} = 001 : X_{1,2} = 1110$$
$$K_{1,3} = 010 : X_{1,3} = 1000$$
$$K_{1,4} = 011 : X_{1,4} = 0000$$
$$K_{1,5} = 100 : X_{1,5} = 1110$$
$$K_{1,6} = 101 : X_{1,6} = 0000$$
$$K_{1,7} = 110 : X_{1,7} = 1010$$
$$K_{1,8} = 111 : X_{1,8} = 1010$$

$$C = 0100$$

$$K_{2,1} = 00 : X_{2,1} = 1000$$
$$K_{2,2} = 01 : X_{2,2} = 1011$$
$$K_{2,3} = 10 : X_{2,3} = 1010$$
$$K_{2,4} = 11 : X_{2,4} = 1001$$
$$K_{2,5} = 11 : X_{2,5} = 1001$$
$$K_{2,6} = 11 : X_{2,6} = 1001$$
$$K_{2,7} = 11 : X_{2,7} = 1001$$
$$K_{2,8} = 11 : X_{2,8} = 0011$$

The values of X that match are: $(X_{1,3}, X_{2,1})$, $(X_{1,7}, X_{2,3})$ and $(X_{1,8}, X_{2,3})$. This indicates the keys are either: $(K_{1,3} = 010, K_{2,1} = 000)$, $(K_{1,7} = 110, K_{2,3} = 010)$ or $(K_{1,8} = 111, K_{2,3} = 010)$. To know which keys, then try with the second plaintext/ciphertext pair.

$$P = 1111$$

$$K_{1,3} = 010 : X_{1,3} = 1100$$

$$X_{1,3} = 1100$$

$$K_{2,1} = 000 : C_{2,1} = 1110$$

The ciphertext obtained (`1110`) does not match the expected value (`1101`). Hence this set of keys is incorrect. Now try the next set:

$$P = 1111$$

$$K_{1,7} = 110 : X_{1,7} = 1001$$

$$X_{1,7} = 1001$$

$$K_{2,3} = 010 : C_{2,7} = 1101$$

We have a match. Lets check the final set:

$$P = 1111$$

$$K_{1,8} = 111 : X_{1,8} = 1101$$

$$X_{1,8} = 1101$$

$$K_{2,3} = 010 : C_{2,3} = 0001$$

No match. That means the keys must be $K_{1,7} = 110$ *and* $K_{2,3} = 010$. *That is,* $K = 110010$.

Question 3 [4 marks]

(a) Consider the cipher ABC (Table 1) being used in Counter Mode to act as a pseudorandom number generator. If the initial value of the counter is 0 (decimal) and the seed is 3 (decimal), then what are the first 12 pseudorandom bits? [3 marks]

Bits: _____

Answer. *In Counter mode, the counter value is encrypted with the cipher, where the seed is the key. The pseudorandom bits are the output ciphertext. Then the counter is incremented and encrypted with the same seed to produce more bits, and so on.*

$$Seed = 011$$

$$Counter = 0000$$

$$Randombits = 1010$$

$$Counter = 0001$$

$$Randombits = 0011$$

$$Counter = 0010$$

$$Randombits = 1011$$

So the 12 pseudorandom bits are: 101000111011.

(b) What is the maximum period, in bits, of the above PRNG? [1 mark]

Answer. *Once the counter reaches 1111 it will then wrap back to 0000. So there are 16 possible input values, then the ciphertext will repeat. So the psuedorandom sequence consists of 64 bits.*

Question 4 [12 marks]

(a) The one-time pad is considered to be *unconditionally secure*. What does unconditionally secure mean? [1 mark]

Answer. *Even with unlimited resource/time, the cipher is unbreakable, i.e. attacker cannot determine correct plaintext given a ciphertext.*

(b) Explain the weakness of the Vigenère cipher. [1 mark]

Answer. *For long plaintexts, repetition of the key leads to structure in the ciphertext that the attacker can take advantage of to determine the plaintext.*

(c) 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 what type? [1 mark]

Answer. *Chosen plaintext attack*

(d) Consider the following commands run in Linux (and assume no errors in running the commands):

```
$ echo -n "stevengordonabcd" > file1.txt
$ openssl enc -aes-256-ofb -in file1.txt -out file2.txt -nopad
-K f27036fbb28e554d6b3a5d8ae68e6423 -iv fd8a418a301fdca8ffa9f8e7305e60df
```

i. How many bits in the file `file2.txt`? [1 mark]

Answer. *128 bits. There are 16 characters, each stored as 8 bits.*

ii. How many attempts, on average, needed to perform a brute force attack on the ciphertext? [1 mark]

Answer. 2^{255}. *AES with a 256 bit key is used.*

iii. What mode of operation was used? [1 mark]

Answer. *Output Feedback Mode*

(e) What is the name of the concept that aims to reduce the statistical nature of input plaintext in the output ciphertext of a block cipher? [1 mark]

Answer. *Diffusion*

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

Answer. *With steganography, other users do not know that you are communicating something secret.*

(g) Explain a disadvantage of a 64-bit ideal block cipher. [1 mark]

Answer. *The key length would need to be* 64×2^{64} *bits, which is too large to store and distribute.*

(h) 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 10^9 messages per second. In theory, what is the average time to apply a brute force attack on this One Time Pad when a message is 200 characters? [1.5 marks]

Answer. $16^{200}/10^9/2$ *seconds.*

(i) 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]

Answer. *Method 1: Take a plaintext* P *and key* K_1 *and find the ciphertext* C_1*. Now modify the key by one bit to get* K_2 *and encrypt to get* C_2*. Count the number of bits which are different in the ciphertext. Repeat for different keys, and average the number of bits that differ. For the cipher to exhibit the avalanche effect, you'd expect to see the average number of bits that differ to be half of the block size. Method 2: same as method 1 but instead of modifying the key, modify the plaintext.*

Question 5 [5 marks]

(a) Two security services are *confidentiality* and *authentication*. List and describe two other security services. [2 marks]

Answer. *Access Control: Prevent unauthorised use of a resource. Data Integrity: Assure data received are exactly as sent by authorised entity. Nonrepudiation: Protect against denial of one entity involved in communications of having participated in communications. Availability: System is accessible and usable on demand by authorised users according to intended goal.*

(b) Describe the difference between a *passive* and *active* attack on security. [1 mark]

Answer. *A passive attack does not modify the system or network resources (when compared to normal operation without an attack), whereas an active attack does.*

(c) Describe two types of passive attacks. [2 marks]

Answer. *Release message contents: malicious user intercepts messages and obtains their contents. Traffic analysis: malicious user observes patterns of communications between users.*

Question 6 [4 marks]

(a) Decrypt the ciphertext *QDESWYARPEZY* with keyword *secretpassword* using the Playfair cipher. [4 marks]

Answer: _____

Answer. *Write the keyword in the Playfair matrix, filling with remaining letters of the alphabet:*

`s e c r t`

`p a w o d`

`b f g h i`

`k l m n q`

`u v x y z`

Now break the ciphertext into digrams. Then read the plaintext for each digram from the Playfair matrix:

- $QD \rightarrow it$
- $ES \rightarrow st$
- $WY \rightarrow ox$
- $AR \rightarrow oe$
- $PE \rightarrow as$
- $ZY \rightarrow yx$

Giving the plaintext: itstoxoeasyx. Removing the padding in too *and the final* x *gives: Its too easy.*

Question 7 [3 marks]

(a) If the output of `E/P` in the first round of S-DES is `10001101` and K_1 is `01101001`, then what is the output of `P4` in the first round? [3 marks]

Answer: _____

Answer. *Output of E/P XOR with K_1: 10001101 XOR 01101001 = 11100100. Left half, 1110, is input to S-Box S0. Row 10 and column 11 gives: 11. Right half, 0100, is input to S-Box S1. Row 00 and column 10 gives: 10. The input to P4 is 1110. The output is: 1011.*

Question 8 [4 marks]

Calculate the following, showing calculations and assumptions. Answers without calculations will receive 0 marks.

(a) $\phi(24)$ [1 mark]

Answer. *Factors of 24 are: 1, 2, 3, 4, 6, 8, 12, 24. Numbers less than 24 that have gcd with 24 equal to 1 are: 1, 5, 7, 11, 13, 17, 19, 23. Therefore the answer is: 8.*

(b) Multiplicative inverse of 7 in (mod 15) [1 mark]

Answer. $7 \times 13 = 91$*;* $91 \bmod 15 = 1$*; therefore the multiplicative inverse of 7 is 13.*

(c) $43267^{1873} \bmod 1961$ [2 marks]

Answer. *Here we will try to use Euler's theorem. If we assume* $n = 1961$*, then to use Euler's theorem, then* $\phi(1961)$ *must equal* 1872*. Does it? If we recognise that the two prime factors of* 1961 *are* 37 *and* 53*, then* $\phi(1961)$ *can be calculated as* $(37-1) \times (53-1)$ *which is* 1872*. Hence Euler's theorem can be applied, giving the answer of* 43267*.*

Question 9 [6 marks]

Consider a general Caesar cipher that uses the English lowercase letters, as well as two other characters—a space and a full stop. For mapping to numbers, the letters come first (i.e. $a = 0$), followed by space character and then finally the full stop (.) character. For example, the plaintext:

`This is an example.`

is valid as it uses only characters from the available set.

(a) Write an equation for decrypting ciphertext C to obtain plaintext P using this cipher. [1 mark]

Answer.

$$P = (C - K) \bmod 28$$

(b) How many possible keys does this cipher have? [1 mark]

Answer. *28*

(c) The following ciphertext was obtained by encrypting plaintext P, a three word sentence, with the above cipher. What is the key and plaintext? [4 marks]

`brsaisaipcxj`

Plaintext: _____

Key: _____

Answer. *First the key must be determined. The hint is that the plaintext is a three word sentence. That means there must be two spaces, and so two letters in the ciphertext must be the same. There are three letters in the ciphertext that occur two times:* `s`*,* `a` *and* `i`*. Since the space character maps to number 26, the possible keys are:*

- `s=18`*: K=20, since* $(26 + 20) \bmod 28 = 18$
- `a=0`*: K=2, since* $(26 + 2) \bmod 28 = 0$
- `i=8`*: K=10, since* $(26 + 10) \bmod 28 = 8$

Unfortunately the letters all appear in reasonable positions to be spaces (an unreasonable position would be two letters together—its unlikely the plaintext has two spaces next to each other). So one option is to try all three above keys. But it is expected that if it is a sentence then it will finish with a full stop (27). The last ciphertext letter is `j=9`*. This suggests the key is 10, since* $(27 + 10) \bmod 28 = 9$*. So lets try K=10.*

`Ciphertext: b r s a i s a i p c x j`

```
Ciphertext:  01 17 18 00 08 18 00 08 15 02 23 09
Minus 10 :  19 07 08 18 26 08 18 26 05 20 13 27
Plaintext:  t h i s _ i s _ f u n .
```

This is fun.

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
```

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

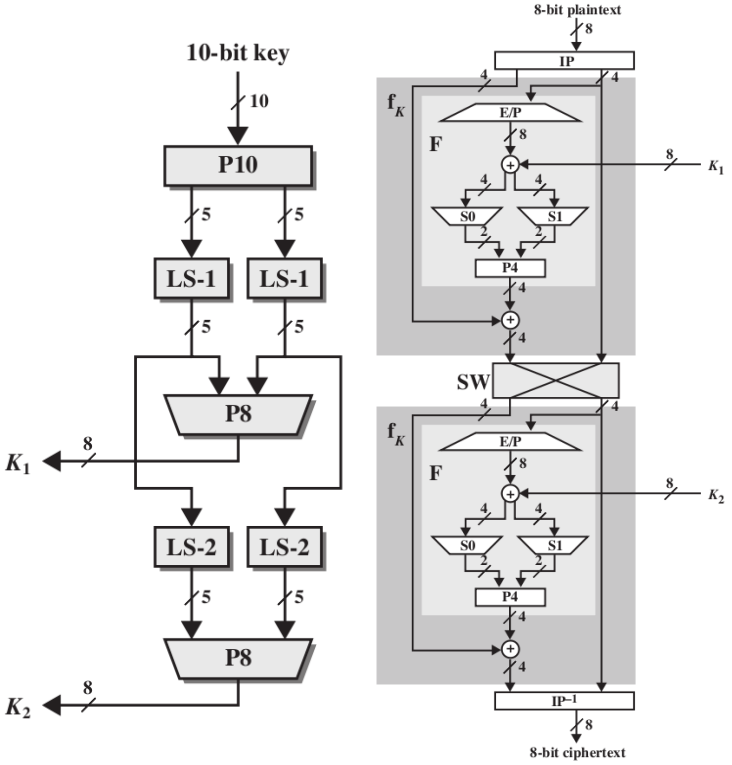


Figure 1: S-DES Key Generation and Encryption

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.

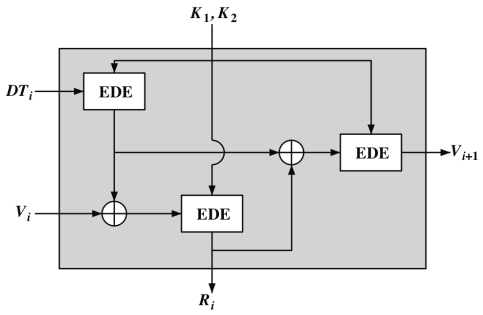
Linear Congruential Generator

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

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

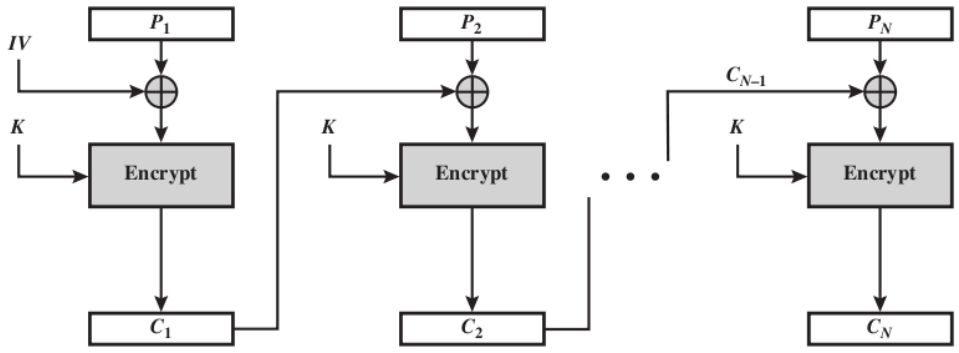


Figure 2: CBC mode of operation

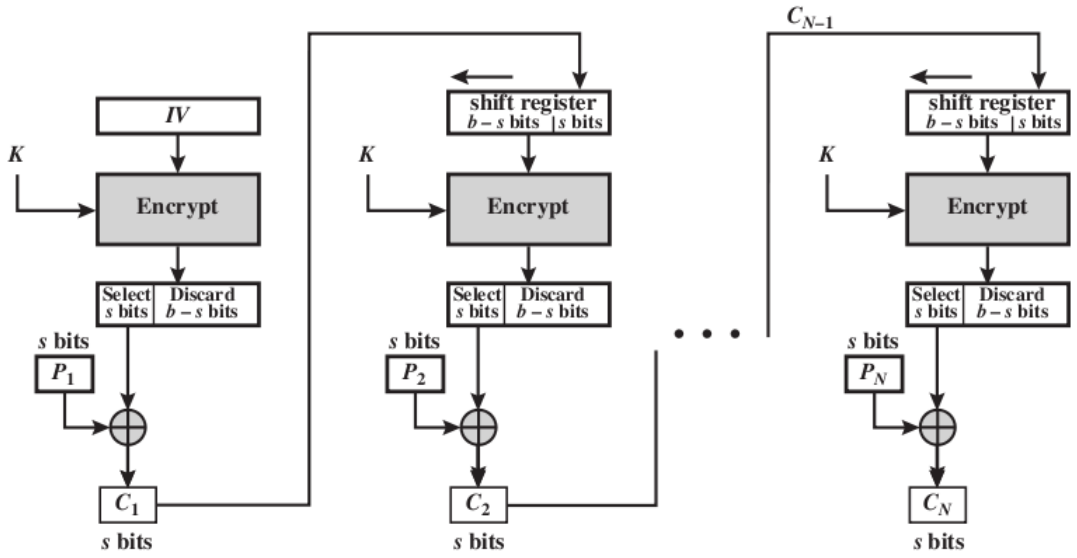


Figure 3: CFB mode of operation

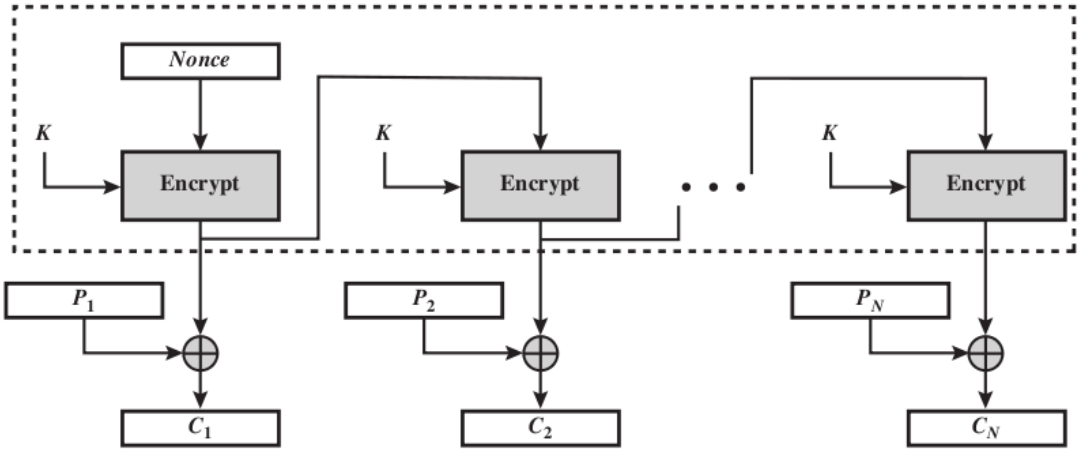


Figure 4: OFB mode of operation

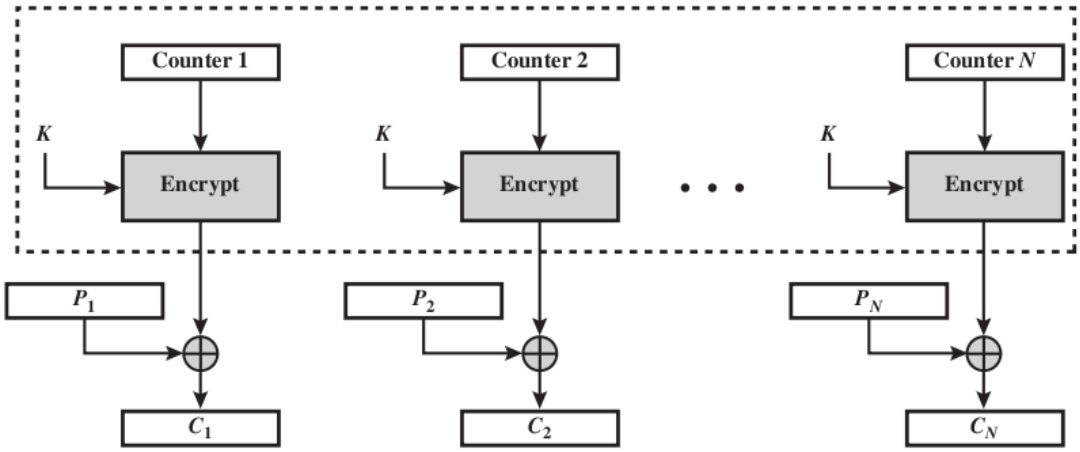


Figure 5: CTR mode of operation