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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam Answers: 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).

Security and Cryptography, Semester 2, 2011

Prepared by Steven Gordon on 23 February 2012
CSS322Y11S2E01, Steve/Courses/2011/S2/CSS322/Assessment/Midterm-Exam.tex, r1619

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) *OpenSSL* 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 *AES or IDEA or Blowfish or . . . .*

(c) The Feistel structure for block ciphers achieves security by using multiple rounds, where in each round it alternates between *substitutions* 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 *chosen ciphertext.*

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

(f) *Non-repudiation* 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 *an active* attack.

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

(i) *Base64* 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 *XOR* operation on the input stream of *ciphertext* and a keystream.

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

(l) The *one-time pad* is considered unconditionally secure.

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

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

(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 $2x$ seconds.

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

(q) A modification attack is an attack against the *data integrity* service.

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

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

(t) A challenge with *symmetric* 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: ____

Answer. *If Thanaruk sent the message confidentially to Steve, then that means Thanaruk encrypted M using Steve's public key. So he performed:*

$$C = M^e \bmod n$$

which is:

$$3 = M^{61} \bmod 437$$

To find M you must solve a discrete logarithm:

$$61 = dlog_{M,437}(3)$$

Although this is solvable (with a computer), using a calculator in the exam would be very hard. Lets consider another approach. We also know that:

$$M = C^d \bmod n$$

but do not know d. To find d we need to know $\phi(437)$ since d is the multiplicative inverse of $e = 61$ in $\bmod \phi(437)$. Manually finding $\phi(437)$ will take a long time in the exam, so instead factor $n = 437$ into its two prime factors. Try to divide 437 by prime numbers 3, 5, 7, 11, and so on will tell you that $19 \times 23 = 437$. That is, $p = 19$ and $q = 23$. Therefore $\phi(437) = 18 \times 22 = 396$. Now find the multiplicative inverse of 61 in $\bmod 396$. You can quickly find that:

$$61 \times 13 = 2 \times 396 + 1$$

and therefore $d = 13$. Now returning to the decryption:

$$M = 3^{13} \bmod 437$$

$$M = 147$$

Therefore the plaintext, M, is 147.

(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]

Answer.

- *Factoring n into its prime factors p and q*
- *Manually determining $\phi(n)$ without knowing p and q*
- *Solving a discrete logarithm to find d directly*

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: ______________________________

Answer. *37, 49 and 22*

(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]

Answer. *m; it should be prime and as large as possible for computer*

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: ____

Answer. *The secret value is calculated by:*

$$K = Y_{Steve}^{X_{you}} \bmod q$$

which is:

$$K = 2^{10} \bmod 19$$

i.e. $K = 17$

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

Answer: ____

Answer. *Steve calculated* Y_{Steve} *as:*

$$Y_{Steve} = \alpha^{X_{Steve}} \bmod q$$

which is:

$$2 = 3^{X_{Steve}} \bmod 19$$

Therefore 3 to the power of some number, X_{Steve}*, mod 19 equals 2. Lets try brute force:*

$$3^1 \bmod 19 = 3$$

$$3^2 \bmod 19 = 9$$

$$3^3 \bmod 19 = 8$$

$$3^4 \bmod 19 = 6$$

$$3^5 \bmod 19 = 15$$

$$3^6 \bmod 19 = 7$$

$$3^7 \bmod 19 = 2$$

Therefore $X_{Steve} = 7$.

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: ____

Answer. *Note that even though there are 4 cores available, Triple-DES cannot be parallelized across the cores, because the input of one DES encryption depends on the output of the previous, i.e. serial operations. Simiarly, with CBC the input to one block encryption depends on the output of the previous, i.e. serial operations.*

DES and Triple-DES (3DES) operate on 64-bit, or 8-Byte, blocks. A plaintext of 8KB contains 1000 blocks. Each DES encryption of a block takes 10us. In 3DES, DES is used three times, meaning each block takes 30us. Therefore the total time is 30,000us or 30ms.

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

Answer: ____

Answer. *Similar to above, but now the block encryptions can be parallelized. In CTR the encryption of one block does not depend on the previous block having been encrypted. That is, parallel operations are possible. With four cores available there is a speed-up of 4 times compared to using a single core as in CBC above. Hence the encryption time is 7.5ms.*

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: ____

Answer. *With CBC when decrypting a block of ciphertext, the previous block of ciphertext is used. The 11th block of ciphertext has a bit error. Therefore the first 10 blocks would decrypt to the correct plaintext. But obviously the 11th block would not produce the correct plaintext because the input ciphertext is wrong. Also, the next block would not decrypt to the correct plaintext because the previous ciphertext block is wrong. And so on. The 11th block and all subsequent blocks would produce the wrong plaintext. Hence 10 out of 1000 plaintext blocks would be correct (or 80B out of 8000B).*

(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: ____

Answer. *With OFB when decrypting a block of ciphertext the previous block of ciphertext is NOT used. Hence the first 10 blocks will decrypt to the correct plaintext. The 11th block will not, as the input ciphertext is wrong. The subsequent blocks will decrypt to the correct plaintext. So 999 out of 1000 blocks (or 7992B out of 8000B) will decrypt to the correct plaintext.*

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]

Answer. *With OFB if using the same key and with the same nonce value, then the output from the encrypt stage (before XOR with plaintext) will always be the same for each file. Hence if you have two different files but they have an identical block in identical positions, then the corresponding output ciphertext block will be the same. The attacker could use this pattern to assist in determining the output from the encrypt block (in particular if the attacker had a known plaintext-ciphertext pair).*

With CBC even if two files have an identical block in the identical position, the output ciphertext will be different since it depends on the previous blocks. Hence it is recommended to change the Nonce value for OFB for each encryption of a file.

Question 6 [8 marks]

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

Answer: ____

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

g e n i u

s a b c d

f h k l m

o p q r t

v w x y z

Now break the plaintext into digrams, padding with x at the end. Then read the ciphertext for each digram from the Playfair matrix:

- *sh* → *AF*
- *an* → *BE*
- *no* → *GQ*
- *nx* → *BN*

Giving the ciphertext: AFBEGQBN.

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

Answer: ____

Answer. *The keyword has 5 characters, meaning there are 5 columns and therefore 4 rows. Write the ciphertext in columns:*

i v s r e

s h m t a

r n d i a

e m n l a

Now re-arrange the columns so that the 4th becomes the 1st, the 1st becomes 2nd, 2nd becomes 3rd, 5th becomes 4th and 3rd becomes 5th:

r i v e s

t s h a m

i r n a d

l e m a n

The plaintext is rivestshamirnadleman, i.e. Rivest, Shamir (n = and) Adleman of RSA fame.

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]

Answer. *A one-to-one mapping means each input plaintext letter produces a unique ciphertext letter.*

(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]

Answer. *Any value relatively prime with 26 and greater than 3. E.g. 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.*

(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]

Answer. *Any value greater than 3 and less than 26 that is not relatively prime with 26, e.g. 4, 6, 8, 10, 13, 14, 16, 18, 20, 22, 24.*

(d) Using the syntax MI(a) for the multiplicative inverse of a, write an equation for the decryption operation of the Affine Caesar cipher. [3 marks]

Answer.

$$p = \mathrm{D}([a,b],C) = \mathrm{MI}(a)(C-b) \bmod 26$$

(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]

Answer. *For a one-to-one mapping a must have a multiplicative inverse in* mod *n. That is true if a and n are relatively prime. The number of numbers relatively prime with n (and less than n) is $\phi(n)$.*

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]

Answer.

- *Method 1. Take a plaintext P and key K and encrypt P using both A and B to obtain Ca1 and Cb1. Now change P by a single bit (using the same K), encrypt to obtain Ca2 and Cb2. Compare the number of bits different in Ca1-Ca2 and Cb1-Cb2. Repeat this process for many different plaintexts and then compare the average number of bits in ciphertext between both algorithms.*
- *Method 2. Same as Method 1 except instead of changing a bit in the plaintext, change a bit in the key.*

(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]

Answer. *Perform multiple encryptions (using different keys and plaintexts) and:*

- *Test 1. Count the number of 1's and 0's in the output. Should be equal number.*
- *Test 2. Select an M-bit block of the output and perform Test 1.*
- *Test 3. Count the length of sequences of 1's (and similar for 0's) the lengths should be small.*

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: ____

Answer. *First note that there are 28 characters in the ciphertext. As there was no padding used on the rail-fence cipher then the original plaintext had 28 characters. The depth of the rail-fence must therefore be a factor of 28, e.g. 2, 4, 7, 14. Lets consider these 4 depths in the following.*

We know the first 8 characters of plaintext are security. *When using the rail-fence cipher on this plaintext then the letters will be arranged according to the depth. That is the output from the rail-fence will be as follows (where the uppercase letters are unknown; different uppercase letters are used for each row):*

- *Depth 2:* `scrtAAAAAAAAAAeuiyBBBBBBBBBB`
- *Depth 4:* `srAAAAAeiBBBBBctCCCCCuyDDDDD`
- *Depth 7:* `syAAeBBBcCCCuDDDrEEEiFFFtGGG`
- *Depth 14:* `sAeBcCuDrEiFtGyHIIJJKKLLMMNN`

Now we know the ciphertext was obtained from one of the above using a 4 character Vigenere keyword, lets say WXYZ.

Consider depth 2 and apply Vigenere:

```
P: s c r t A A A A A A A A A A e u i y B B B B B B B B B B
K: W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z
C: k z i k g w p x a v g b e n k m v x a n m c g v l a k g
```

Converting to numbers and looking at two known plaintext characters (s and i) where the same key letter (W) is used we get the equations:

$$(18 + W) \bmod 26 = 10$$

$$(8 + W) \bmod 26 = 21$$

There is no value of W that solves the above two equations (first equation W = 18, second equation W = 13). Therefore a depth of 2 for the rail-fence is incorrect.

Now try depth 4.

```
P: s r A A A A A e i B B B B B c t C C C C C u y D D D D D
K: W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z W X Y Z
C: k z i k g w p x a v g b e n k m v x a n m c g v l a k g
```

For plaintext letters s and i, we get the equations:

$$(18 + W) \bmod 26 = 10$$

$$(8 + W) \bmod 26 = 0$$

W = 18 solves both equations. Now lets try plaintext letters r and u:

$$(17 + X) \bmod 26 = 25$$

$$(20 + X) \bmod 26 = 2$$

X = 8 solves both equations. Now lets try plaintext letters c and y:

$$(2 + Y) \bmod 26 = 10$$

$$(24 + Y) \bmod 26 = 6$$

Y = 8 solves both equations. Now lets try plaintext letters e and t:

$$(4 + Z) \bmod 26 = 23$$

$$(19 + Z) \bmod 26 = 12$$

Z = 19 solves both equations.

So with a rail-fence with depth 4, the keyword 18, 8, 8, 19 or ***siit*** *produces the correct ciphertext for the first known plaintext letters. If we now try to decrypt the entire ciphertext with this keyword:*

```
C: k z i k g w p x a v g b e n k m v x a n m c g v l a k g
K: s i i t s i i t s i i t s i i t s i i t s i i t s i i t
P: s r a r o o h e i n y i m f c t d p s u u u y c t s c n
```

And now apply the rail-fence of depth 4:

```
s r a r o o h
 e i n y i m f
  c t d p s u u
   u y c t s c n
```

Gives the plaintext: securityandcryptoissomuchfun. As the plaintext makes sense (and within the context, so does the keyword) we have been successful. There is no need to try depths 7 and 14 (although if you do you'll find there is no solution, as with depth 2).

Security and crypto is so much fun.

(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`

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

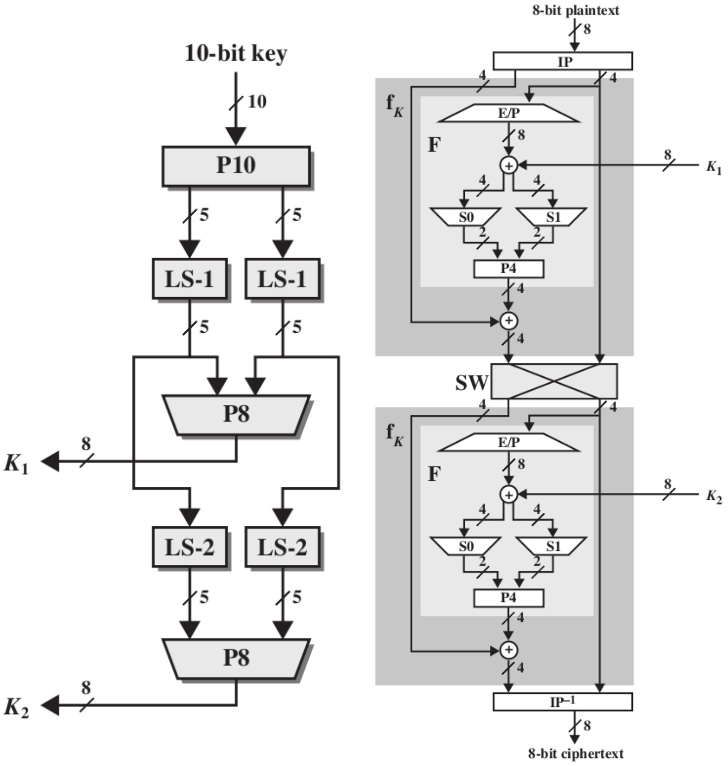


Figure 1: S-DES Key Generation and Encryption

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

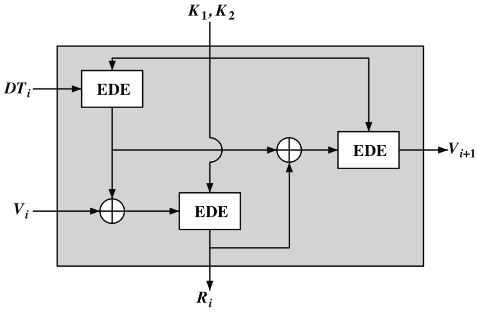
Linear Congruential Generator

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

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

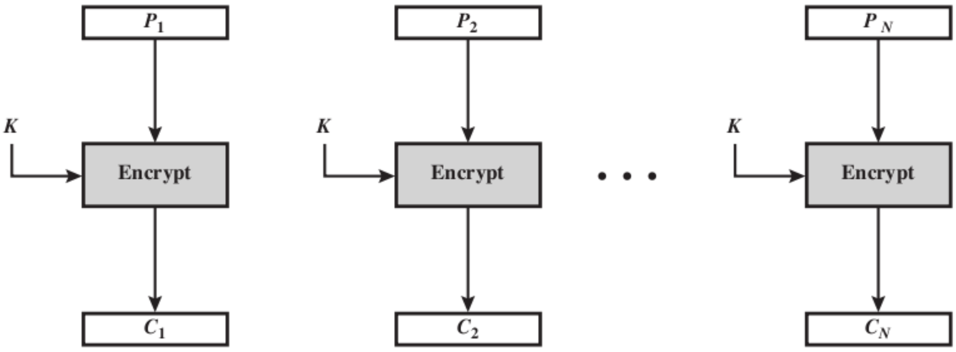


Figure 2: ECB mode of operation

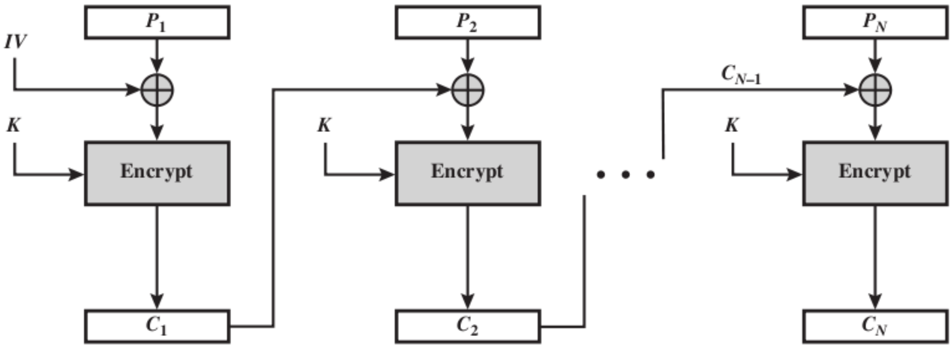


Figure 3: CBC mode of operation

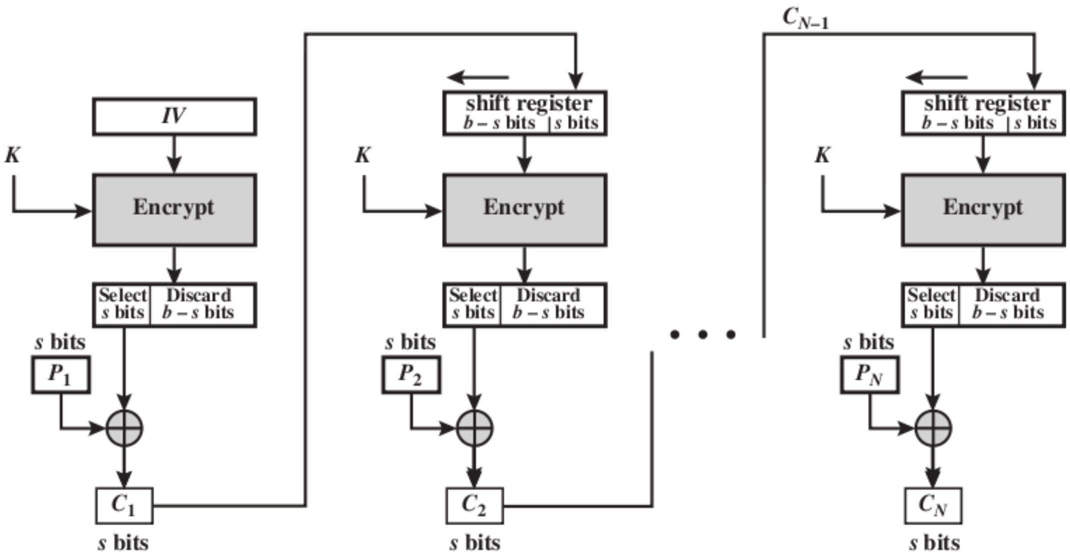


Figure 4: CFB mode of operation

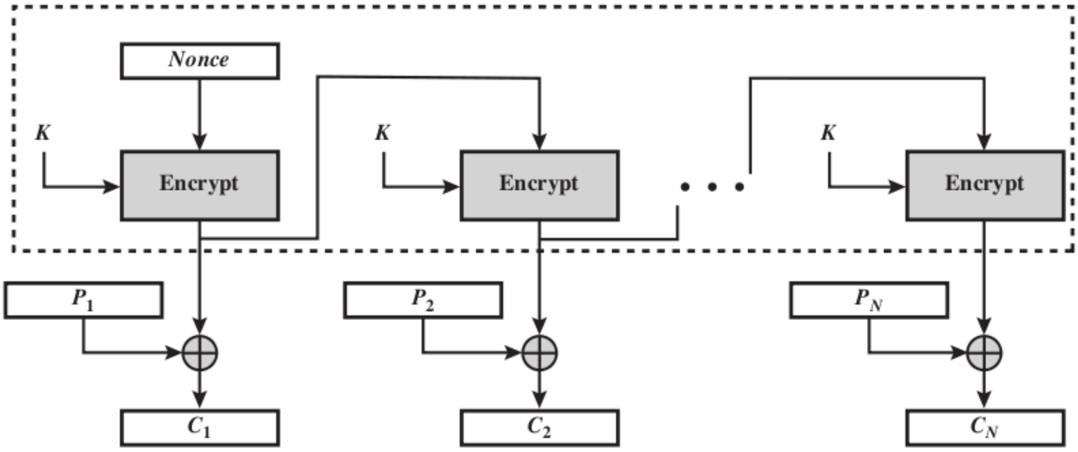


Figure 5: OFB mode of operation

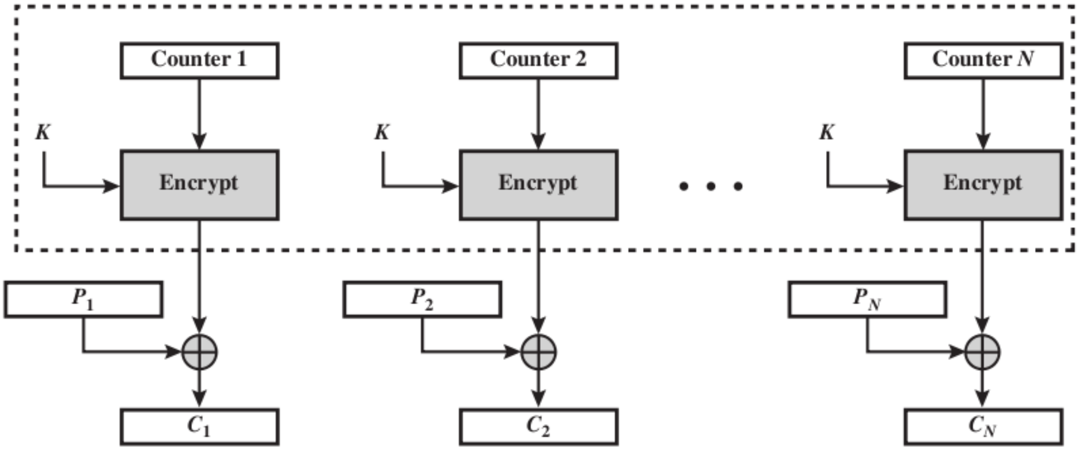


Figure 6: CTR mode of operation