Kenny Ta
Jose Gomez

CECS 378 Assignment 2 - Cryptography

20 points

Assignment Description. Answer the following questions from the Chapter 2, 20, and 21 readings from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both of your names on each submission.

1. How many keys are required for two people to communicate via a symmetric cipher?

Only one encryption key is required.

2. What is a message authentication code?

A small block of data that is generated using a secret key. This is used to make sure that no alterations were made to the message.

3. What are the principal ingredients of a public-key cryptosystem?

The key ingredients are: plaintext. Encryption algorithm, public and private key, ciphertext, and decryption algorithm.

4. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted *C*1 (Figure 20.6, pg. 622 in CSPaP) obviously corrupts *P*1 and *P*2.

(a) Are any blocks beyond *P*2 affected?

Yes, because C_{n-1} *is XORed with* P_n . This means that any errors in a block will propagate in all the remaining blocks.

(b) Suppose that there is a bit error in the source version of *P*1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

This means that there will be errors in all the remaining blocks. When the receiver decrypts the message, it won't make sense.

5. You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure 20.11 on pg. 632 in CSPaP shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:

(a) For security?

If we are talking about security, then we would use 3DES because it is very resistant to cryptanalysis. The use of it's 168-bit key length makes it harder to brute-force crack.

(b) For performance?

If we are talking about performance, then we would use DES. DES's algorithm requires ⅓ of 3DES's algorithm calculations to perform, thus making 3DES slower.

(c) And answer why for each.

For security we would choose 3DES because it has a larger key and making it harder to brute-force. For performance we would use DES because 3DES has more 3x as much calculations, making it slower than DES.

6. Fill in the remainder of this table:

Mode	**Encrypt**	**Decrypt**
ECB	$C_j = E(k, P_j) \quad where\, j = 1, ..., N$	$P_j = D(k, C_j) \quad where\, j = 1, ..., N$
CBC	$C_1 = E(K[P_1 \oplus IV])$ $C_j = E[K, [P_j + C_{j-1}])$ $where\, j = 2, .., N$	$P_1 = D(K, C_j) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1}$ $where\, j = 2, ..., N$
CFB	$C_1 = P_1 \oplus S_s[E(K, IV)]$	$P_1 = C_1 \oplus S_s[E(K, IV)]$

CTR	$C = P_1 \oplus E[Counter_j]$ $where\ j = 1, ..., N$	$P_j = D(E[Counter_j]) \oplus C_1$ $where\ j = 1, ..., N$

7. Padding may not always be appropriate. For example, one might wish to store the encrypted data in the same memory buffer that originally contained the plaintext. In that case, the ciphertext must be the same length as the original plaintext. A mode for that purpose is the ciphertext stealing (CTS) mode. Figure 20.12a on pg. 633 in CSPaP shows an implementation of this mode.

C - cypher text
P - plain code
K - key
IV - initialization vector

(a) Explain how it works.

The first block is XORed with the initialization vector and plain text. Then the key gets added to the encryption to create the ciphertext block. Then every iteration after, the next plain text block gets XORed with the encrypted coded block's select leftmost bits before it.

(b) Describe how to decrypt C_{n-1} and C_n.

To decrypt the received ciphertext, C_{n-1} and C_n is passed through the decryption algorithm where the IV is XORed with the preceding ciphertext block to produce the plaintext block.

8. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?

It is possible because the Feistel cipher is the general structure used by all other ciphers. Therefore we can use the hash function to combine with one subkey or the IV to be XORed. The hash function that does this combining is always in the same direction(one-way), therefore making it possible for both encryption and decryption.

9. Perform encryption and decryption using the RSA algorithm for the following:

(a) $p = 3$; $q = 11$, $e = 7$, $M = 5$

N = pq = 33

ϕ (n) = (p-1)(q-1) = 20

de mod 20 = 1 and d < 20 so d = 3

Public key (pu) = {e, n} = {7, 33}

Private key (pr) = {d,n} = {3, 33}

Encryption: C = M^e mod n

C = 5^7 mod 33 = 14

Decryption: M = C^d mod n

M = 14^3 mod 33 = 5

(b) *p* = 5; *q* = 11, *e* = 3, *M* = 9

N = pq = 55

φ (n) = (p-1)(q-1) = 4*10 = 40

d(3) mod 40 = 1 and d < 40 so d = 27

Public key (pu) = {e, n} = {3, 55}

Private key (pr) = {d,n} = {27, 55}

Encryption: C = M^e mod n

C = 9^3 mod 55 = 14

Decryption: M = C^d mod n

M = 14^27 mod 55 = 9

(c) *p* = 7; *q* = 11, *e* = 17, *M* = 8

N = pq = 77

φ (n) = (p-1)(q-1) = 60

de mod 60 = 1 and d < 60 so d = 53

Public key (pu) = {e, n} = {17, 77}

Private key (pr) = {d,n} = {53, 77}

Encryption: C = M^e mod n

C = 8^17 mod 77 = 57

Decryption: M = C^d mod n

M = 57^53 mod 77 = 8

(d) *p* = 11; *q* = 13, *e* = 11, *M* = 7

N = pq = 143

ϕ (n) = (p-1)(q-1) = 120

d(11) mod 120 = 1 and d < 120 so d = 11

Public key (pu) = {e, n} = {11, 143}

Private key (pr) = {d,n} = {11, 143}

Encryption: C = M^e mod n

C = 7^11 mod 143 = 106

Decryption: M = C^d mod n

M = 106^11 mod 143 = 7

(e) *p* = 17; *q* = 31, *e* = 7, *M* = 2

N = pq = 527

ϕ (n) = (p-1)(q-1) = 480

de mod 480 = 1 and d < 480 so d = 343

Public key (pu) = {e, n} = {7, 527}

Private key (pr) = {d,n} = {343, 527}

Encryption: C = M^e mod n

$C = 2^7 \bmod 527 = 128$

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

$M = 128^{343} \bmod 527 = 2$

10. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume *n* = *pq; e* is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with *n*. Does this help us in any way?

If both ‘e’ and ‘n’ are known, then only ‘d’ would be needed to decrypt the message. To find ‘d’, math based attacks could be used, with the given information.