Breesy Reyes
Sam Chen

Assignment 2 - Cryptography

1. **How many keys are required for two people to communicate via a symmetric cipher?**
   Only one key is required

2. **What is a message authentication code?**
   A secret key that generates a small block of code that is appended to the message.

3. **What are the principal ingredients of a public-key cryptosystem?**
   The client must create a pair of public and private keys. User ID must be attached to the public key. Unsigned certificate must be given to a certificate authority. The certificate authority creates a hash function to calculate the hash code of the unsigned certificate. A digital signature to attach to a signed certificate.

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 C1 (Figure 20.6, pg. 622 in CSPaP) obviously corrupts P1 and P2.**
   (a) **Are any blocks beyond P2 affected?**
   No only P1 and P2 will be affected.

   (b) **Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?**
   All ciphertext will depend only on P1. If there is a bit error in plain text P1 then it will affect the cipher text of C1. At the receiver the decryption algorithm will fix the correct plan text for blocks except the one with the error.

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?**
   CBC mode for the initialization vector. It determines the number of bits compared to a 1 loop from brute force attacks. The initialization vectors are kept secret in the 3DES algorithm to build the block encryption in CBC mode.

   (b) **For performance?**

A new cipher text block is created every 1 tick in the three loop 3DES, which is opposite of the single loop DES because it creates the cipher text every 3 ticks. The three loop DES would be 3 times faster than the one loop DES.

(c) And answer why for each.

6. **Fill in the remainder of this table:**

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

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.**

   (a) Explain how it works.

   Using CBC technique we encrypt the first N-2 blocks. We use the XOR operation between C_{N-2} and P_{N-1} to create Y_{N-1}. Pad PN with zeroes at the end with XOR with EN-1 to create YN. To create C_{N-1}. we have to encrypt Y_N

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

   Decrypt the cipher text of C_{N-1}. with the k value and the result will be of the XOR operation with cipher text of C_{N-1}. P_N || X = (C_N || 00...0) + D(K,[C_N - 1])
   For C_N you must decrypt cipher text of C_n with the k value, use XOR for C_{N-2}. C_{N-1} + D(K, [C_N || X])

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?**

   We have two 32 bit L and R halves are used in DES
   $L_i = R_{i-1}$
   $R_i = L_{i-1} + F(R_{i-1}, K_i)$

In DES the function F is $F(K_{AB},M)$ and maps a 32 bit R and 48 bit K into a 32 bit output. There is also a one way function F and XOR. Since the function F maps to an 80 bit input into a 32 bit output it will be a one way function. So any hash function produced 32 bit output is used in the function F.

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

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

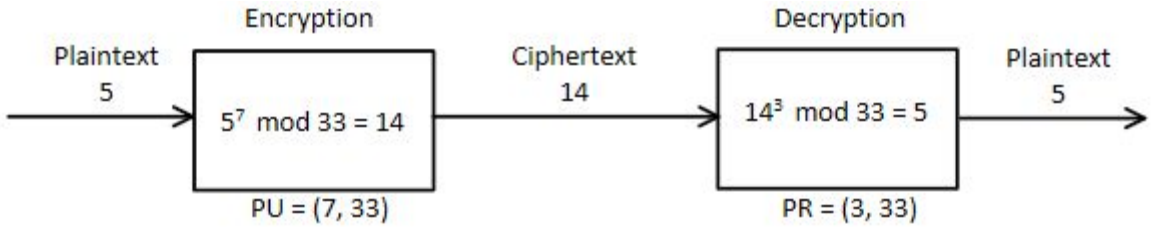
1. p and q are prime numbers
2. n = p * q = 3 * 11 = 33
3. Φ(n) = (p - 1)(q - 1) = 2 * 10 = 20
4. GCD:

   20 = 7 * 2 + 6
   7 = 6 * 1 + 1
   6 = 1 * 6 + 0

   GCD = 1

   1 = 7 - 6
   1 = 7 - (20 - 7 * 2)
   1 = 7 - 20 + 7 * 2
   1 = - 20 + 7 * 3

   d = e^{-1} mod Φ(n) = e^{-1} mod 20 = 3 mod 20 = 3
5. 5^7 mod 33 = [(5^4 mod 33)(5^2 mod 33)(5^1 mod 33)] mod 33 = [31 * 25 * 5] mod 33 = 14
6. 14^3 mod 33 = [(14^2 mod 33)(14^1 mod 33)] mod 33 = [14 * 31] mod 33 = 5



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

1. p and q are prime numbers
2. n = p * q = 5 * 11 = 55
3. Φ(n) = (p - 1)(q - 1) = 4 * 10 = 40
4. GCD:

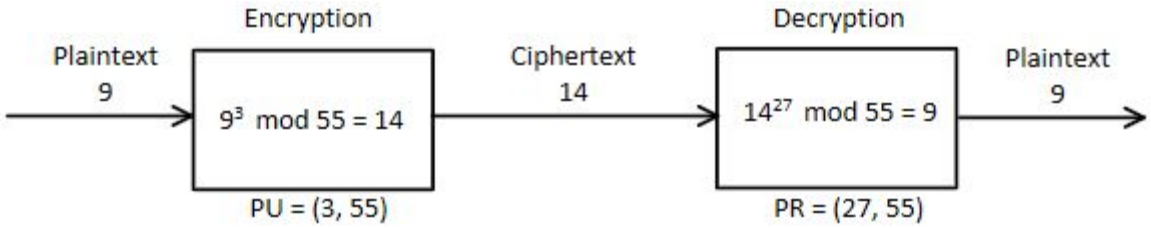
   40 = 13 * 3 + 1
   13 = 1 * 13 + 0

   GCD = 1

   1 = 40 - 3 * 13

   d = e^{-1} mod Φ(n) = e^{-1} mod 40 = -13 mod 40 = (27 - 40) mod 40 = 27
5. 9^3 mod 55 = [(9^2 mod 55)(9^1 mod 55)] mod 55 = (26 * 9) mod 55 = 14

6. 14^{27} mod 55 = [(14^{8} mod 55)(14^{8} mod 55)(14^{4} mod 55)(14^{4} mod 55)(14^{2} mod 55)(14^{1} mod 55)] mod 55 = (14 * 31 * 26 * 26 * 16 * 16) mod 55 = 9



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

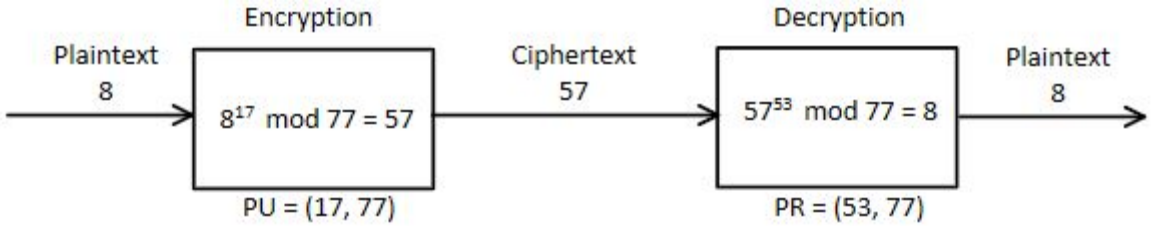
1. p and q are prime numbers
2. n = p * q = 7 * 11 = 77
3. Φ(n) = (p - 1)(q - 1) = 6 * 10 = 60
4. GCD:

   60 = 17 * 3 + 9
   17 = 1 * 9 + 8
   8 = 1 * 8 + 0

   GCD = 1

   1 = 9 - 8
   1 = 9 - (17 - 9)
   1 = 60 - 17 * 3 - (17 - 60 + 17 * 3)
   1 = 60 - 17 * 3 + 60 - 17 * 4
   1 = 60 * 2 - 17 * 7

   d = e^{-1} mod Φ(n) = e^{-1} mod 60 = -7 mod 60 = (53 - 60) mod 60 = 53
5. 8^{17} mod 77 = [(8^{8} mod 77)(8^{4} mod 77)(8^{2} mod 77)(8^{2} mod 77)(8^{1} mod 77)] mod 77 = [71 * 15 * 64 * 64 * 8] mod 77 = 57



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

1. p and q are prime numbers
2. n = p * q = 11 * 13 = 143
3. Φ(n) = (p - 1)(q - 1) = 10 * 12 = 120
4. GCD:

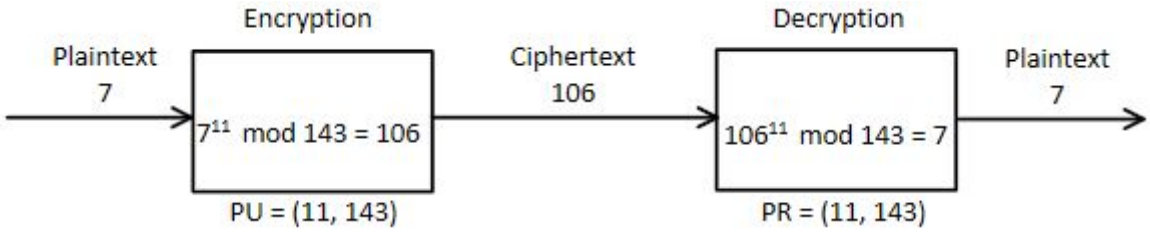
   120 = 11 * 10 + 10
   11 = 10 * 1 + 1
   10 = 1 * 10 + 0

   GCD = 1

1 = 11 - 10
1 = 11 - (120 - 11 * 10)
1 = 11 -120 + 11 * 10
1 = -120 + 11 * 11

d = e^{-1} mod Φ(n) = e^{-1} mod 120 = 11 mod 120 = 11

5. 7^{11} mod 143 = [(7^4 mod 143)(7^4 mod 143)(7^2 mod 143)(7^1 mod 143)] mod 143 = (113 * 113* 49* 7) mod 143 = 106



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

1. p and q are prime numbers
2. n = p * q = 17 * 31 = 527
3. Φ(n) = (p - 1)(q - 1) = 16 * 30 = 480
4. GCD:

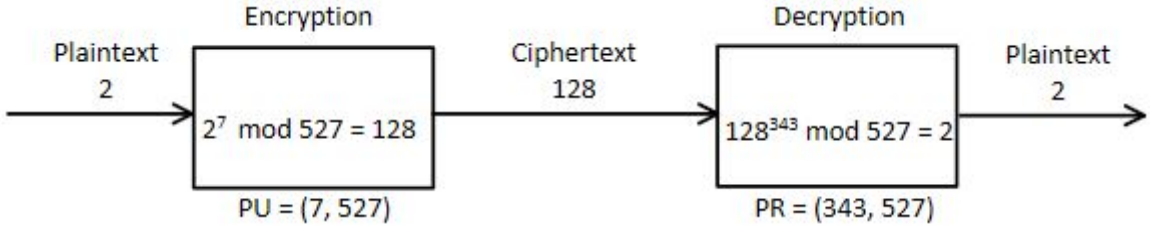
480 = 7 * 68 + 4
7 = 4 * 1 + 3
4 = 1 * 3 + 1
3 = 1 * 3 + 0

GCD = 1

1 = 4 - 3
1 = 4 - (7 - 4)
1 = 4 - (7 - (480 - 7 * 68))
1 = 4 - (7 - 480 + 7 * 68)
1 = 480 -7 * 68 - 7 + 480 -7 * 68
1 = 480 * 2 - 7 * 137

d = e^{-1} mod Φ(n) = e^{-1} mod 480= -137 mod 480 = (343 - 480) mod 480 = 343

5. 2^7 mod 527 = [(2^4 mod 527)(2^2 mod 527)(2^1 mod 527)] mod 527= [16 * 4 * 2] mod 527= 128



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?**
    Yes, it helps us. If m has a common factor with n, the factor should be p or q and the cipher text should have the same common factor with n. If m is a prime number, it has to be p or q. If not, the gcd(n, m) is p or q.