Yuvika Nibber

Assignment 2

1. For symmetric cipher, we need n(n-1)/2 keys where n is the number of keys. For 2 people, 2(2-1)/2 = 1. Therefore, only 1 key is required.
2. Message authentication code (MAC) is a security key between two parties that share a common secret. It creates a secret message that helps for communication. This is untampered data between the two parties.
3. The principal ingredients of a public key cryptosystem are plaintext, encryption and decryption algorithm, public keys, and private keys and ciphertext.
4. A. No, only P1 and P2 will be affected.

B. The ciphertext will be different from the original ciphertext because all the ciphertexts are dependent on p1. The receiver will get an error, but the plaintext does not change because it is not included in the decipher.

1. A. one loop CBC for security

B. three loop CBC for performance

C. One loop is more secure because it makes attack more difficult than a simple loop whereas three loops is faster because it is more vulnerable. The three look performs decryption and encryption on each loop which makes it faster.

Text, letter

Description automatically generated

1. A. encryption of the first block (N-2) using CBC. Then XOR P(N-1) with the previous cipher block C(N-2) which will create Y(N-1). Y(N-1) will be encrypted to E(N-1).

The first L bytes of E(N-1) will make turn it to C(N). Padding P(N) with 0 at the end and XOR with E(N-1) will turn it to Y(N). Then by encrypting Y(N) we get C(N-1). C(N-1) and C(N) are the last two blocks of the cipher text.

B. Decrypting C(N)= P(N-1) = C(N-2) XOR D (K, [C(N) || X])

Decrypting C(N-1) = P(N) || X = (C(N)|| 00..0) XOR D(K,[C(N-1)]

1. Yes, it is possible to use a hash function to create a block cipher with a structure similar to DES. A DES structure only has F and XOR. DES structure uses 32-bit L and R halves. A hash function uses 32-bit output and uses only F function.
2. p = 3; q = 11, e = 7, M = 5

RSA Encryption Key (7, (311))->(7, 33)

f(n) = (3-1)(11-1)) = (2)(10) = 20

d = (1 + kf(n)e= (1 + 20k7) = 217=3 (for k = 1)

C = Me(mod n) = 57(mod 33) = 14

M = Cd(mod n) = 143(mod 33) = 5

p = 5; q = 11, e = 3, M = 9

RSA Encryption Key (3, (511))->(3, 55)

f(n) = (5-1)(11-1)) = (4)(10) = 40

d = (1 + kf(n)e= (1 + 40k3) = 813=27 (for k = 2)

C = Me(mod n) = 93(mod 55) = 14

M = Cd(mod n) = 1427(mod 55) = 9

p = 7; q = 11, e = 17, M = 8

RSA Encryption Key (17, (711))->(17, 77)

f(n) = (7-1)(11-1)) = (6)(10) = 60

d = (1 + kf(n)e= (1 + 60k17) = -11917=-7 (for k = -2) d = -7(mod 60) = 53

C = Me(mod n) = 817(mod 77) = 57

M = Cd(mod n) = 5753(mod 33) = 8

p = 11; q = 13, e = 11, M = 7

RSA Encryption Key (11, (1113))->(11, 143)

f(n) = (11-1)(13-1)) = (10)(12) = 120

d = (1 + kf(n)e= (1 + 120k11) = 12111=11 (for k =1)

C = Me(mod n) = 711(mod 143) = 106

M = Cd(mod n) = 10611(mod 143) = 7

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

RSA Encryption Key (7, (1731))->(7, 527)

f(n) = (17-1)(31-1)) = (16)(30) = 480

d = (1 + kf(n)e= (1 + 480k7) = -9597=-137 (for k =-2) d = -137(mod 480) = 343

C = Me(mod n) = 27(mod 527) = 128

M = Cd(mod n) = 128343(mod 527) = 2

1. If plaintext blocks have a common factor with n, it will help find a private key. It has n modulo n as a common factor. The encoded blocks in RSA is smaller than the PQ. P and Q are primes and a factor of N, so we know it’s either P or Q. Since the block is a factor, it is used to divide by N.