Home Page: http://www.public.asu.edu/~bhao2

Homework 7

Problems:

1 to 11.

Question: 1

Using the monoalphabetic cipher in Figure 8.3, encode the message "This is an easy problem." Decode the message "rmij'u uamu xyj."

Answer:

"This is an easy problem." -> "uasi si my cmiw lokngch"

"rmij'u uamu xyj." -> "wasn't that fun"

Question: 2

Show that Trudy's known-plaintext attack, in which she knows the (ciphertext, plaintext) translation pairs for seven letters, reduces the number of possible substitutions to be checked in the example in Section 8.2.1 by approximately 10^9.

Answer:

Subtract 7 from total number of letters 26 is 19 -> 19 factorial words can be got. For 26 factorial words, it is difference of approximately 10^9.

Question: 3

Consider the polyalphabetic system shown in Figure 8.4. Will a chosenplaintext attack that is able to get the plaintext encoding of the message "The quick brown fox jumps over the lazy dog." be sufficient to decode all messages? Why or why not?

Answer:

Yes, all messages can be decoded using Caesar cipher. The phrase contains all alphabetical letter, so the decipher is clear.

Question: 4

Consider the block cipher in Figure 8.5. Suppose that each block cipher Ti simply reverses the order of the eight input bits (so that, for example, 11110000 becomes 00001111). Further

suppose that the 64-bit scrambler does not modify any bits (so that the output value of the mth bit is equal to the input value of the mth bit). (a) With n = 3 and the original 64-bit input equal to 10100000 repeated eight times, what is the value of the output? (b) Repeat part (a) but now change the last bit of the original 64-bit input from a 0 to a 1. (c) Repeat parts (a) and (b) but now suppose that the 64-bit scrambler inverses the order of the 64 bits.

Answer:

a. 00000101, 00000101, 00000101, 00000101, 00000101, 00000101, 00000101, 00000101

b. 00000101, 00000101, 00000101, 00000101, 00000101, 00000101, 00000101, 10000101

c. a. 10100000, 10100000, 10100000, 10100000, 10100000, 10100000, 10100000, 10100000

b. 10100001, 10100000, 10100000, 10100000, 10100000, 10100000, 10100000, 10100000

Question: 5

Consider the block cipher in Figure 8.5. For a given "key" Alice and Bob would need to keep eight tables, each 8 bits by 8 bits. For Alice (or Bob) to store all eight tables, how many bits of storage are necessary? How does this number compare with the number of bits required for a full-table 64- bit block cipher?

Answer:

Total Number of bits=number of tables*size of each table*size of each entry

=8*2^8*8= 2^14 bits

2^14 bits are far smaller if compared with the number of bits required for a full-table 64- bit block cipher (2^71).

Question: 6

Consider the 3-bit block cipher in Table 8.1. Suppose the plaintext is 100100100. (a) Initially assume that CBC is not used. What is the resulting ciphertext? (b) Suppose Trudy sniffs the ciphertext. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn't know the specific cipher), what can she surmise? (c) Now suppose that CBC is used with IV = 111. What is the resulting ciphertext?

Answer:

a. 011011011
b. All possible 3 bit combinations can be guessed, thus potentially decrypt the message.

c. 101100110

Question: 7

(a) Using RSA, choose p = 3 and q = 11, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. (b) Repeat part (a) but now encrypt "dog" as one message m.

Answer:

a. n=p*q=3*11=33.

(p-1)(q-1)=(3-1)(11-1)=20

Let e and d to be 9,

e*d-1=9*9-1=80 which is divisible by 20.

Letter	m	m^e	Ciphertext	c^d	M_2	letter
d	4	262144	25	38146972265625	4	d
o	15	38443359375	3	19683	15	o
g	7	40353607	19	322687697779	7	g

b.

Letter	m	m to 5-bit
d	4	00100
o	15	01111
g	7	00111

Dog = 00100011100111 = 4583 = m and m -> n. 8.

Question: 8

Consider RSA with p = 5 and q = 11.

a. What are n and z?

b. Let e be 3. Why is this an acceptable choice for e?

c. Find d such that de = 1 (mod z) and d < 160.

d. Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. Hint: To simplify the calculations, use the fact:

[(a mod n) • (b mod n)] mod n = (a • b) mod n

Answer:

a. n=p*q=5*11=55
   z=(p-1)(q-1)=(5-1)(11-1)=40
b. because it has no common factor with z and it is less than n.
c. d should obey ed – 1 is divisible by z:
   (ed-1)/z = (3*d-1)/40 -> d = 27
d. m^e = 8^3=512
   c = m^e mod n = 512 mod 55 =17

Question: 9

In this problem, we explore the Diffie-Hellman (DH) public-key encryption algorithm, which allows two entities to agree on a shared key. The DH algorithm makes use of a large prime number p and another large number g less than p. Both p and g are made public (so that an attacker would know them). In DH, Alice and Bob each independently choose secret keys, SA and SB, respectively. Alice then computes her public key, TA, by raising g to SA and then taking mod p. Bob similarly computes his own public key TB by raising g to SB and then taking mod p. Alice and Bob then exchange their public keys over the Internet. Alice then calculates the shared secret key S by raising TB to SA and then taking mod p. Similarly, Bob calculates the shared key S´ by raising TA to SB and then taking mod p.

a. Prove that, in general, Alice and Bob obtain the same symmetric key, that is, prove S = S´.

b. With p = 11 and g = 2, suppose Alice and Bob choose private keys SA = 5 and SB = 12, respectively. Calculate Alice's and Bob's public keys, TA and TB . Show all work.

c. Following up on part (b), now calculate S as the shared symmetric key. Show all work.

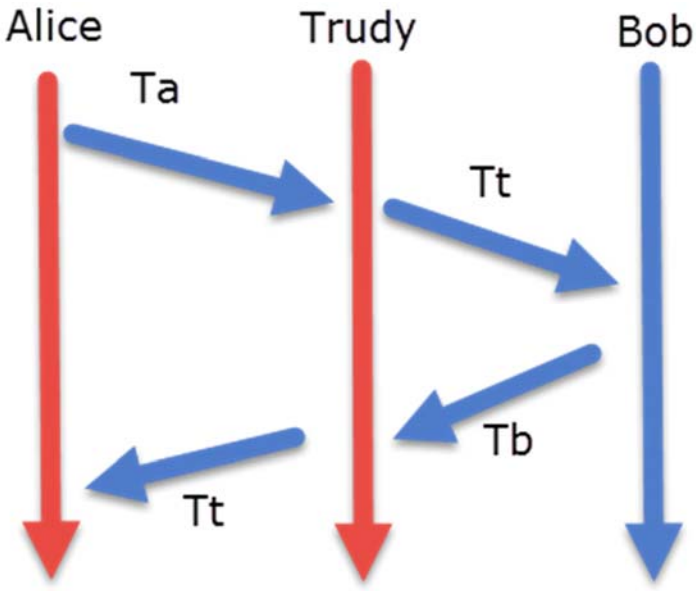
d. Provide a timing diagram that shows how Diffie-Hellman can be attacked by a man-in-the-middle. The timing diagram should have three vertical lines, one for Alice, one for Bob, and one for the attacker Trudy.

Answer:

a. $S = {T_B}^{S_A}\ mod\ p = (g^{S_B S_A}) mod\ p = (g^{S_A} mod\ p)^{S_B} mod\ p = {T_A}^{S_B} mod\ p = S'$
b. For Alice: $v = g^{S_A} mod\ p = 2^5 mod 11 = 10$

   For Bob: $u = g^{S_B} mod\ p = 2^{12} mod\ 11 = 4$

c. $10^5 mod\ 11 = 10$
d.



Question: 10

Suppose Alice wants to communicate with Bob using symmetric key cryptography using a session key KS. In Section 8.2, we learned how public-key cryptography can be used to distribute the session key from Alice to Bob. In this problem, we explore how the session key can be distributed—without public key cryptography—using a key distribution center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by KA-KDC and KB-KDC. Design a scheme that uses the KDC to distribute KS to Alice and Bob. Your scheme should use three messages to distribute the session key: a message from Alice to the KDC; a message from the KDC to Alice; and finally a message from Alice to Bob. The first message is KA-KDC (A, B). Using the notation, KA-KDC, KB-KDC, S, A, and B answer the following questions.

a. What is the second message?

b. What is the third message?

Answer:

a. Alice got the message from KDC and verified it and extracted R1 from that message. She also saved it. She have the one time session key K thus she can extracts $K_{B\text{-}KDC}$ (A, K) and send it to Bob.
b. KB-KDC (A, K) is decrypted by Bob using $K_{B\text{-}KDC.}$ He also could extracts A and K. Right now, Bob got the one time session key K and the person who shared the key. He will perform the authenticating with Alice using K.

Question: 11

Compute a third message, different from the two messages in Figure 8.8, that has the same checksum as the messages in Figure 8.8.

Answer:

I	O	U	1
9	0		9
0	B	O	B