FINAL EXAM

Student Name:

ID:

**Computer Engineering Department**

**College of Computer and Information Sciences**

**Instructor: Dr. Kashif Akhtar Saleem**

**Course Code: CEN 448 Duration: 3 hour**

**Course Name: Security and Internet Protocols Date: July 30, 2013**

**Semester: Summer Semester 1433/1434**

**Section 1**

1. Secret-key cryptography

A Also called asymmetric or unconventional cryptography

B Also called symmetric or conventional cryptography

C Also called systematic or conventional cryptography

1. Cryptanalyst is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A sender B receiver

C skilled decoder D helper

1. Email recipients without S/MIME capability can read message but not verify signature when the following S/MIME type is used:

A enveloped-data B clear-signed data

C signed-data D signed and enveloped data

1. The s-boxes in DES have:

A 64 bit input, 56 bit output B 64-bit input, 48-bit output

C 56-bit input, 48 bit output D 48-bit input, 48 bit output

1. An SSL protocol that provides services to other SSL protocols:

A record protocol B handshake protocol

C change cipher spec protocol D alert protocol

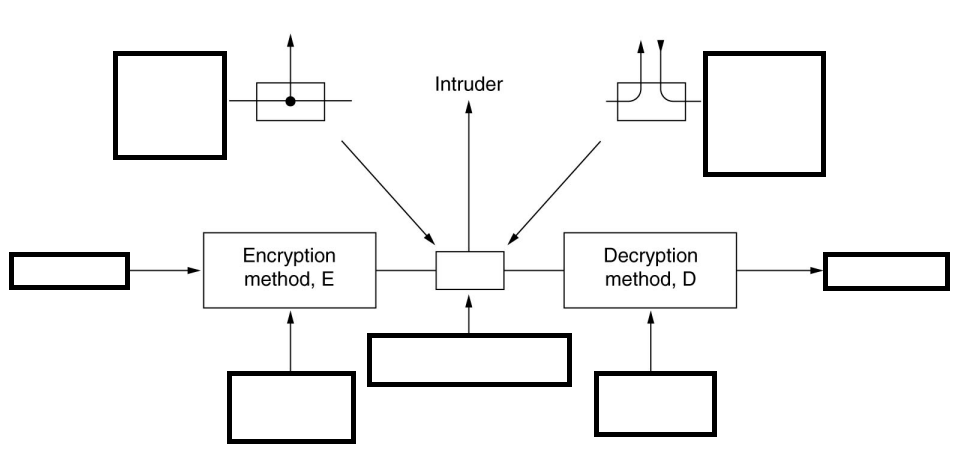
1. Password selection scheme that rejects weak passwords while user is choosing password is called:

A inactive password checking B reactive password checking

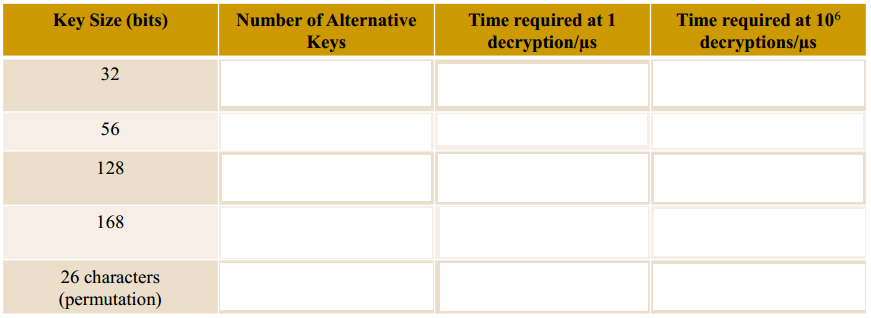
C proactive password checking D defective password checking

**Section 2**

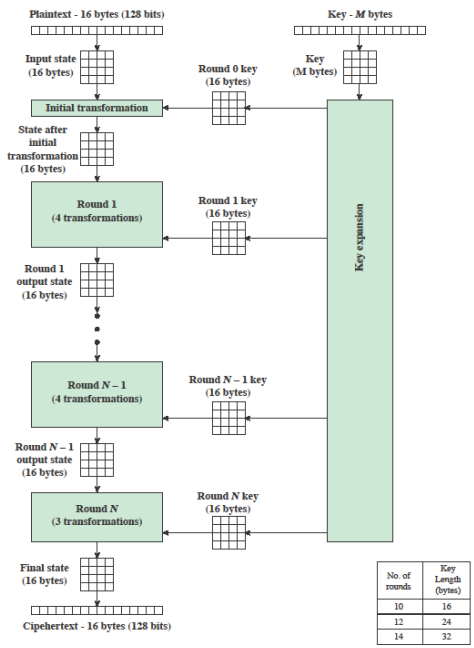
1. Fill the boxes, upper 2 boxes require the type of attacks:



2. Fill the table below, according to column headings



3. What process performed by the following structure and belong to standard?



**Section 3 (Provide answer / Solve any 12 of the following 18 Questions)**

Note: Question 9 and 12 contains 10 marks

1. Compare between a monoalphabetic cipher and a polyalphabetic cipher in terms of speed, cryptanalysis complexity and ease of use.
2. Define the following terms:

a. Confidentiality

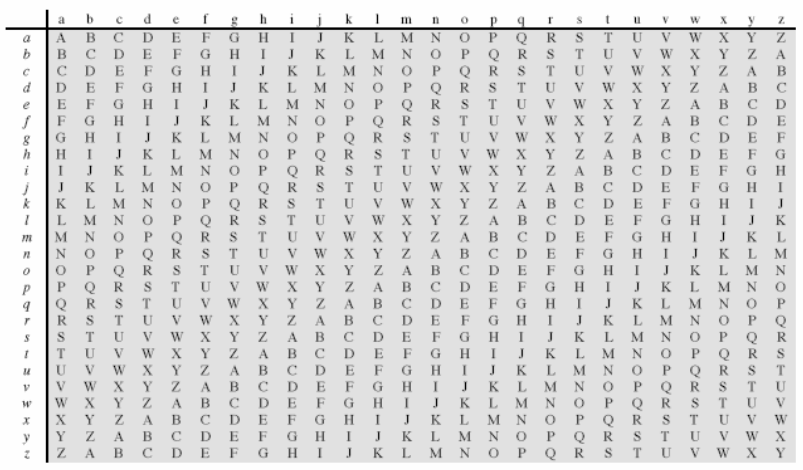
b. Integrity

c. Availability

1. What is the difference between a block cipher and a stream cipher? What type of application for which each of them is more suitable?

|  |  |
| --- | --- |
| block cipher | stream cipher |
|  |  |
|  |  |

1. Show that the round function F in Feistel Cipher does not have to be reversible.
2. What is the minimum key size (in bits) that will make brute force attack infeasible for a computer that can perform 180 decryptions per microsecond? Assume feasible time is 10 days
3. Using the Vigenère cipher, encrypt the word "iwillbeinthestoreatnight" using the key computer.



1. The following ciphertext was generated using Transposition Matrix applied twice.

RJVCEIBOOAMRMNORSSHELEYOESKU

The key used is 5764624. Find the original message, which is an English statement

1. What is the purpose of the S-boxes in DES? Why the DES is currently considered insecure?
2. This problem provides a numerical example of encryption using a one-round version of DES:

Note: This question contains 10 marks

Plaintext

in hexadecimal notation: 93 DF AB C8 37 F2 14 38

in binary notation: 10010011 11011111 10101011 11001000

00110111 11110010 00010100 00111000

Key

Hex 3B 38 98 37 15 20 F7 5E

Binay 00111011 00111000 10011000 00110111

00010101 00100000 11110111 01011110

1. Derive K1, the first-round subkey.
2. Derive L0, R0.
3. Expand R0 to get E[R0], where E[•] is the expansion function of Figure given on next page.
4. Calculate A = E[R0] ⊕ K1.
5. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
6. Concatenate the results of (e) to get a 32-bit result, B.
7. Apply the permutation to get P(B).
8. Calculate R1 = P(B) ⊕ L0.
9. Write down the ciphertext.

This problem must be solved by hand.





1. What is the purpose of the State array?

What is the rationale behind SubBytes and ShiftRows?

1. How does 3DES maintain backward compatibility with DES? Mention the advantages and disadvantages of CBC mode.
2. For the AES key 8C16A62518F868634EE4092BA1E24BBA, calculate AES round keys from w0 up to w7. Show the steps.

Note: This question contains 10 marks

Include left side for calculations and detail steps writeup

1. Perform encryption and decryption using the RSA algorithm, for the following

a. *p* = 4; *q* = 11, *e* = 7; M = 5

b. *p* = 13; *q* = 13, *e* = 12; M = 7

c. *p* = 18; *q* = 41, *e* = 7; M = 2

Note: You must use modular exponentiation for mod calculations and show all steps in written

1. A) What is the difference between authentication and signature?

B) What is the advantage of using message authentication codes over encrypting hash code?

1. Formulate the following problems in terms of security requirements, then suggest the correct procedure to solve each problem:
2. Two people (Ahmed and Badr) would like to communicate with each other. They don’t have any pre-shared secret information. They don’t want other people to spy on their communication.
3. A bank wants to protect its clients when using online banking. Clients tend to use easy passwords. Someone may steal the password and be able to access the client’s account.
4. A bank wants to allow clients to request services on their accounts using email. The bank wants to have a proof that the actual client is the one who sends the email so that they don’t deny it in the future.
5. What is the problem that Kerberos was designed to solve. Explain the network environment and possible threats?
6. Show how SSL can protect against the following attacks:
7. Replay Attack: Earlier SSL handshake messages are replayed.
8. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
9. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.
10. Fill in the following firewall table to satisfy the following constraints:

Allow packets from our hosts to any destination on port 80.

Allow packets from IP address 192.168.100.50 with destination port 25.

Allow all incoming packets to our hosts that are replies to internal packets.

Deny packets that do not match any of the above rules.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| action | src | port | dest | port | flags | comment |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

17

Last Page