

Midterm
CSE 5/7399
Computer System Security
Mark D. Hoffman

Name: Bingying Liang
ID: 48999397

Oct 15 2023

Instructions: Please keep all answers as concise as possible while still conveying all necessary concepts. Please show all necessary work. An extra page is provided in the event that you need more room.

1. Using the following word bank, select fill in the blank with the term most directly related to the concepts below:

Authorization	Authentication	Symmetric Key System
Cipher Text	Kerckhoff's Principle	Plain Text
Public Key System		

- (a) Symmetric Key System Can be used with a Message Authentication Code to provide Integrity to a message.
- (b) Cipher Text The scrambled version of the message in an encryption system.
- (c) Authorization The process of giving someone permission to do or have something. Limited by such technologies as firewalls, Intrusion Detection Systems, and Multilevel Security Systems
- (d) Kerckhoff's Principle The idea that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
- (e) Public Key System Provides the ability to add a secure 'digital signature' to a message.
- (f) Plain Text The original input into an encryption system before modification to obfuscate the message.
- (g) Authentication The process of determining whether someone or something is, in fact, who or what it is declared to be.

2. Briefly describe each of the three components of the C.I.A. Triad including what each is directed at protecting:

Solution: CIA: Confidentiality, Integrity, and Availability.

Confidentiality: prevent unauthorized reading of information, cryptography used for confidentiality.

Integrity: detect unauthorized writing information, cryptography used for integrity.

Availability: Data is available in a timely manner when needed. Availability is a “new” security concern. For example, denial of service(DoS) attacks.

3. A Feistel Cipher is a general format for one possible method of performing a block cipher. Describe the basic flow of a Feistel cipher being sure to include what primary mathematical operator is required to meet this format. (Be able to describe the flow. This can be a flow chart, series of algorithms, or textual description.).

Solution: Feistel Cipher is a type of block cipher, not a specific block cipher.

(a) Split plaintextblock into left and right halves: $P = (L_0, R_0)$.

(b) For each round $i = 1, 2, \dots, n$ compute

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Where F is round function and K_i is subkey

(c) Now can have the Ciphertext: $C = (L_n, R_n)$

4. Compare and contrast Symmetric Key Systems vs. Public Key Systems

Solution: A symmetric key cryptosystem uses the same key to encrypt as to decrypt.

A public key cryptosystem uses a public key to encrypt and a private key to decrypt.

(a) **Key Management: Symmetric Key Systems (SKS):** Only one secret key is used for both encryption and decryption. Both parties (sender and receiver) need to have the same key to communicate securely.

Public Key Systems (PKS): Uses two distinct keys: a public key and a private key. The public key is used for encryption, and the private key is used for decryption. Everyone can know and use a user's public key, but only the user should know their private key.

(b) **Use Cases: Symmetric Key Systems (SKS):** Commonly used for encrypting data at rest (e.g., encrypting files on a hard drive). Often used in session encryption, where a shared secret key is established for a single session.

Public Key Systems (PKS): Typically used for securing data in transit, such as during email or online transactions. Key exchange (e.g., Diffie-Hellman key exchange) and digital signatures.

- (c) **Speed and Efficiency: Symmetric Key Systems (SKS):** Generally faster and requires less computational resources than public key encryption. Efficient for encrypting large amounts of data.

Public Key Systems (PKS): Computationally intensive and slower than symmetric key encryption. Not ideal for encrypting very large amounts of data directly. Instead, often used to encrypt a symmetric key which is then used to encrypt the data.

- (d) **Security: Symmetric Key Systems (SKS):** The main challenge is securely distributing and managing the secret key. If the key is compromised, the data is vulnerable. Both parties must have a trusted method to exchange the secret key without interception.

Public Key Systems (PKS): Since the public key can be freely distributed and only the private key can decrypt the message, there is no need for a secure channel to exchange encryption keys. Vulnerable to specific attacks if not implemented correctly (e.g., man-in-the-middle attacks if public keys aren't properly verified).

5. a. What are the three primary components of Public Key Infrastructure?

Solution: Certificate Authority (CA), Registration Authority (RA), Digital Certificates

- b. Briefly describe one of the primary PKI Trust Models.

Solution: One of the primary PKI Trust Models: Oligarchy.

- i. Multiple trusted CAs: In this model, instead of just one CA being universally trusted (as in a strict hierarchical model), multiple independent CAs are trusted. Each of these CAs can issue, validate, and revoke certificates.
- ii. This is approach used in browsers today: Modern web browsers and operating systems come with a built-in set of trusted root certificates, often referred to as the trust store.
- iii. Certificate Validation: When user visit a secure (HTTPS) website, the website provides its SSL/TLS certificate for validation.
- iv. Browser may have 80 or more certificates, just to verify certificates: The trust store might contain certificates from dozens (often 80 or more) of trusted CAs from around the world.
- v. User can decide which CAs to trust: Advanced users can view and modify the trust store. This means they can decide to trust a new CA by importing its root certificate, or they can revoke trust from a pre-existing CA by removing its certificate.

6. Solve the following modular arithmetic problems:

$$\begin{array}{ll} 12 \bmod 9 = & -4 \bmod 9 = \\ 11^{-1} \bmod 8 = & 4^{-1} \bmod 9 = \\ & 49 \bmod 5 = \end{array}$$

Solution: (a) $12 \bmod 9 = 3$

(b) $-4 \bmod 9 = 4$

(c)

$$\begin{aligned}\therefore (11 \times \frac{1}{11}) \bmod 9 &= 1 \\ \therefore (11 \times 5 \bmod 9) &= 55 \bmod 9 = 1 \\ \therefore \frac{1}{11} \bmod 9 &= 5 \bmod 9 = 5 \\ \therefore 11^{-1} \bmod &= 5\end{aligned}$$

(d)

$$\begin{aligned}\therefore (4 \times \frac{1}{4}) \bmod 9 &= 1 \\ \therefore (4 \times 7) \bmod 9 &= 28 \bmod 9 = 1 \\ \therefore \frac{1}{4} \bmod 9 &= 7 \bmod 9 = 7 \\ \therefore 4^{-1} \bmod 9 &= 7\end{aligned}$$

(e) $49 \bmod 5 = 4$

7. Using the following word bank, select fill in the blank with the term most directly related to the Hashing concepts below:

Compression	Efficiency	One-Way
Weak Collision Resistance		Strong Collision Resistance
Avalanche Effect		Cyclic Redundancy Check

- (a) One-Way Given a value (y) it is infeasible to find a corresponding value (x) such that $h(x) = y$
- (b) Efficiency Should be computationally easy to compute $h(x)$ for any value of x
- (c) Compression Requirement of all hash functions that the resulting output be significantly smaller than the given input
- (d) Cyclic Redundancy Check Form of non-cryptographic hash function that has been improperly used as a method to secure the Wired Equivalency Protocol (WEP)
- (e) Strong Collision Resistance given x and $h(x)$, infeasible to find any x and y , with $x^1 y$ such that $h(x) = h(y)$
- (f) Weak Collision Resistance given x and $h(x)$, infeasible to find $y^1 x$ such that $h(y) = h(x)$
- (g) Avalanche Effect a change to 1 bit of input should affect about half of output bits

8. Using a Shift Cipher with a key of 5, solve the following substitution cipher:

Ymj fsxbjw yt szrgjw knaj nx Inkknj-Mjqqrfs.

Solution:

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shift	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Therefore, “Ymj fsxbjw yt szrgjw knaj nx Inknj-Mjqqrfs.” → “the answer to number five is diffie-hellman.”

9. During the first round of a DES encryption cycle, the 32-bits of R_0 are found to be:

$$R_0 = 00000000000000000010101001100100$$

This is ran through the expansion permutation box [E] below to generate 48-bit $E(R_0)$ Find $E(R_0)$.

Expansion Permutation (E)					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Solution:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	0	0	

Use the Expansion Permutation(E), can get:

32	1	2	3	4	5
0	0	0	0	0	0
4	5	6	7	8	9
0	0	0	0	0	0
8	9	10	11	12	13
0	0	0	0	0	0
12	13	14	15	16	17
0	0	0	0	0	0
16	17	18	19	20	21
0	0	0	1	0	1
20	21	22	23	24	25
0	1	0	1	0	0
24	25	26	27	28	29
0	0	1	1	0	0
28	29	30	31	32	1
0	0	1	0	0	0

$$i.e. : E(R_0) =$$

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0	0

Therefore, $E(R_0) = \underline{00000000000000000000000000000101010100001100001000}$

10. For this same iteration of DES, K_1 is found to be:

$$K_1 = 010011110110110100110101001010101111110110101011$$

Using the solution, $E(R_0)$, from the previous question, and K_1 find the 48-bit input for the S-Boxes, (B).

Solution:

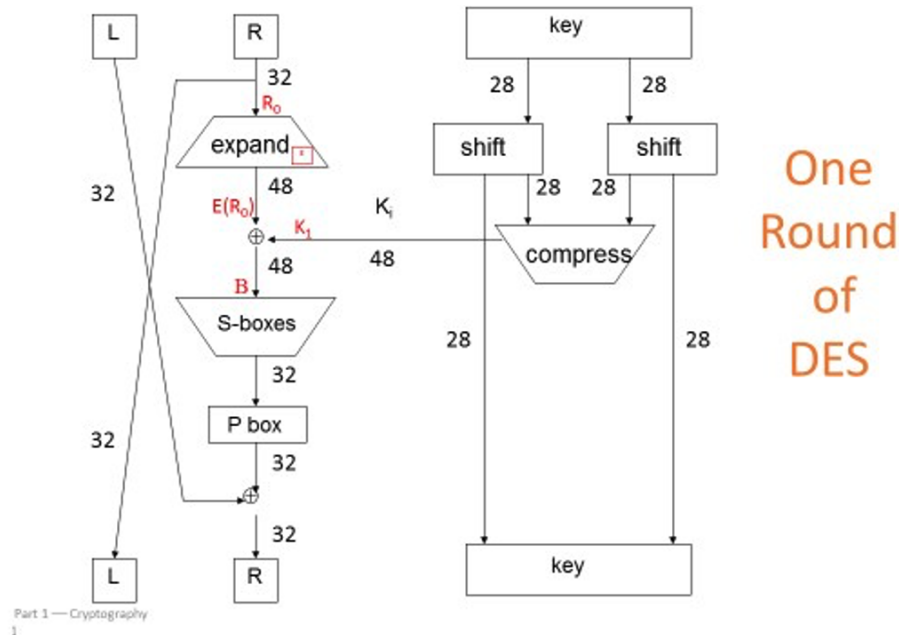
$$\begin{array}{r} E(R_0) : 0000000000000000000000000000000000000000000000000000000 \\ K_1 : 010011110110110100110101001010101111110110101011 \\ \hline E(R_0) \oplus K_1 : 0100111101101101001101010011111111011111010100011 \end{array}$$

Therefore, the 48-bit input for the S-Boxes, (B) is:

B = 010011110110110100110101001111111011111010100011

11. Using the solution, B, from the previous question, determine the proper input and solution to S-Box, S₁ below:

		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00		1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01		0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10		0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11		1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101



Solution:

From the previous question, the proper input is

$B_1 = \underline{01001111011011010011010100111111011111010100011}$

Group the 48-bit result into sets of 6 bits:

010011 110110 110100 110101 001111 111011 111010 100011

For 010011: row = 01, col = 1001, from S-Box is : 0110

For 110110: row = 10, col = 1011, from S-Box is : 0111

For 110100: row = 10, col = 1010, from S-Box is : 1001

For 110101: row = 11, col = 1010, from S-Box is : 0011

For 001111: row = 01, col = 0111, from S-Box is : 0001

For 111011: row = 11, col = 1101, from S-Box is : 0000

For 111010: row = 10, col = 1101, from S-Box is : 1010

For 100011: row = 11, col = 0001, from S-Box is : 1100

Therefore, the solution to S-Box is:

$S_1 \text{ Output} = \underline{0110\ 0111\ 0011\ 0001\ 0000\ 1010\ 1100}$

12. Given the example below, generate a unique key pair by selecting p , q , N , e , and d (DO NOT USE ANY OF THE VALUES LISTED BELOW FOR p or q)

□ Example of RSA

- Select "large" primes $p = 11$, $q = 3$
- Then $N = pq = 33$ and $(p - 1)(q - 1) = 20$
- Choose $e = 3$ (relatively prime to 20)
- Find d such that $ed = 1 \pmod{20}$
 - We find that $d = 7$ works

□ Public key: $(N, e) = (33, 3)$

□ Private key: $d = 7$

Solution: (a) Select "large" primes $p = 17$, $q = 7$

(b) Then $N = pq = 119$ and $(p - 1)(q - 1) = 96$

(c) Choose $e = 5$ (relatively prime to 96)

(d) Find d such that $ed = 1 \pmod{96} = 1$, can find $d = 77$ works. $77 \times 5 = 385 \pmod{96} = 1$

Therefore:

$P = \underline{17}$, $q = \underline{7}$, $N = \underline{119}$, $e = \underline{5}$, $d = \underline{77}$

Extra Work (to be turned in with Exam).