Cryptography Exam Questions

Chapter 1: Introduction

2007:

it cares about 3 topics -> 1. Secuirty attacks, 2-Security Mechanisms, 3- Security Services

1. OSI arch. page 7
2. security attacks page 13 active & passive, and explain each.
3. security services page 17 they are services of defending other companies
4. security mechanisms page 19 methods for defending the system.
5. rasma zay page 21 :S :S kanet moseeba:S:S

Lost Security Exams:

1. Security Attacks
2. Security Services
3. Security Mechanisms

Questions + Sol:

1. Attacks: Passive and Active

Exam Qs Compilation:

1. Compare active attack to passive attack, giving an example for each

Chapter 2: Classical Encryption Techniques

2010 Credit:

1. Play Fair (encrypt keyword)
2. Why Stream Cipher is not recommended to use same key?// Could be Ch.6

2021:

1. What is the one-time pad cryptosystem? What is it used for?
2. What is the main drawback of the one-time pad?
3. You can encrypt 220 values in 1 second:
    a. If the key is 40 bits long:
        i. ■ How long does it take to break it?
        ii. ■ Mention a scenario where it's practical, another one where it's not practical.
    b. If the key is 80 bits long:
        i. ■ How long does it take to break it?
        ii. ■ Mention a scenario where it's practical, another one where it's not Practical.
4.
5. Playfair question (key = monarchy).

2021 Extended:

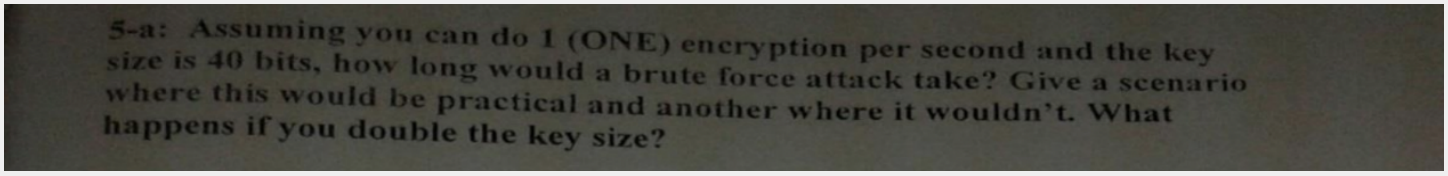
1. What is the one-time pad cryptosystem? What is it used for?
2. What is the main drawback of the one-time pad?
3. You can encrypt 2^20 values in 1 second:
    a. If the key is 40 bits long:

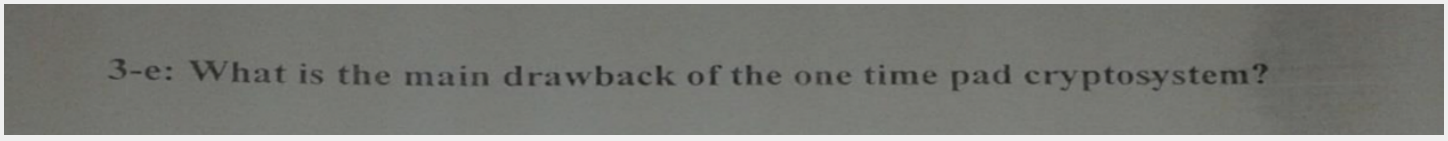
i. ■ How long does it take to break it using brute force attack?
ii. ■ Mention a scenario where it's practical, another one where it's not practical.

b. If the key is 80 bits long:
i. ■ How long does it take to break it?
ii. ■ Mention a scenario where it's practical, another one where it's not Practical.

4. Explain Rail fence cipher, encrypt a plaintext using key (...)
5. Playfair question (key = monarchy).

2015:





2014:

1. what is the disadvantage of the one pad time cryptosystem?

2010:

1. If you have a machine that do 2^20 operation per second, and you are using a 40 bit key, how long will it take to break the key by brute force? Repeat for a 80 bit key? When each key is better to use?

2. Problem on playfair

2010-2:

1. Playfair cipher encrypt University using worldcup
2. Why Stream Cipher is not recommended to use same key?

2010-Chapter:

1. Using a playfair matrix (It was drawn in the exam), encode the word “university” and show your steps Clearly.
2. Why is it not good to encrypt two plain texts using the same key in stream ciphers? // Could be Ch. 6
3. Playfair cipher encrypt University using worldcup
4. Why Stream Cipher is not recommended to use same key?

2010-Credit*:

1. Play Fair (encrypt keyword)
2. Why Stream Cipher is not recommended to use same key? // Ch. 6?

2007:

1. el vigenere attack page 45
2. One time pad page 48
3. Rotor machines(IMP) how does it work.. page 51
4. Steganography
5. 53w awel 54 goom ennena nektebhom w neshra7 w el drawbacks bayen w keda
6. affine caesar cipher

Lost Security Exams:

1. Playfair, Veginere, One-time pad
2. Steganography
3. Why Stream Cipher is not recommended to use same key?

Questions + Sol:

1. (Final 2007) Using this Playfair matrix

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

Encrypt this message:
Must see you over Cadogan West. Coming at once.

1. Define Cryptanalysis and Brute-force attacks
2. Using a playfair matrix, encode the word “university” using the key “worldcup” and show your steps
3. clearly.

Exam Qs Compilation:

1. Arabic rotor machine 29 characters , 4 rotors... how many different
2. substitutions?why?
3. if 6 rotors „how many diff. subs and why?
4. Playfair cipher
5. Rotor machine

6. Steganography (Definition only)

- Using this Playfair matrix

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

- encrypt this message:
- Must see you over Cadogan West. Coming at once.

Chapter 3: Block Ciphers & DES

2010 Credit:

1. Draw Round of DES

2021:

1. DES one round (sketch).

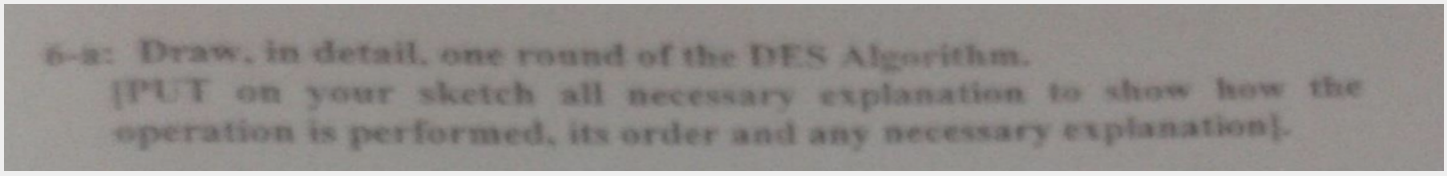
2021 Extended:

1. Draw one round of DES.

2017:

1. Single round of DES

2015:


6-a: Draw, in detail, one round of the DES Algorithm.
[PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].

2010-Credit*:

1. Draw Round of DES

2007:

1. diffusion and confusion: page 67
2. ta2reban el points elly f a7'er 68 w 69 gaat (not sure)
3. el rasma page 74

4. el rasma page 77
5. el example 3ala el S blocks elly f page 78 geh zay ma hwa... bta3 el efgh..., defghi...
6. el avalanche effect page 80

Lost Security Exams:

1. DES
2. SBOX
3. Avalanche Effect
4. Timing Attack
5. Diffusion
6. Confusion

Questions + Sol:

1. What is meant by a timing attack? Compared with brute force attack.

Exam Qs Compilation:

1. Single round DES figure
2. DES key exchange figure* Ch. 10?
3. p.72 data encryption standard
4. Draw the diagram p.77 and discuss their functionalities
5. there was also a question about the Avalanche effect
6. What is meant by a timing attack? Compare with brute force attack.

Chapter 4: Number Theory & Finite Fields Basics

2010 Credit:

1. Smallest number multiplied by 7 to get (2 mod 5) 7aga kda
2. bardo

2021:

1. Which of the following is reducible in GF(2):
   - ◯ X^3 + X^2 + 1
   - ◯ X^3 + 1
   - ◯ All of the above
   - ◯ None of the above

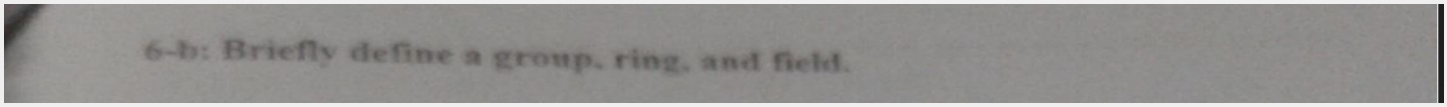
2021 Extended:

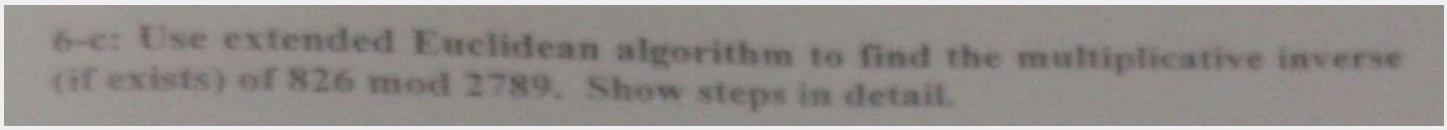
1. Find (polynomial) mod (polynomial) in GF(2)
2. MCQ:
   a. ◯ Which of the following is reducible in GF(2):
      i. ■ X^3 + X^2 + 1
      ii. ■ X^3 + 1
      iii. ■ All of the above
      iv. ■ None of the above
3. Gcd of 4321 and 1234 is?

2017:

1. Get multiplicative inverse arkam (nfs arkam final 2015 bs hwa fe final 2015 mtgaweb 3'lt)

2015:





2014:

1. Compute the GCD of the Two Following Polynomial?
    a. x**4+x**3+x and x***2+1 over GF(2)
2. 2x**3+x**2+2 and x**2+x+1 over GF(3)

3. Compute the Multiplicative inverse of the following F(x) and G(x) in module GF(2^8) x**5+x**4+x2+1 in GF (2**8) with m(x)= x**8+x**4+x**3+x+1

2010-Credit*:

1. Smallest number multiplied by 7 to get (2 mod 5) 7aga kda bardo

2007:

1. el rasma elly f page 100.. lel tafre2 been el group w el field w ....kan el matlob elfar2 benhom bas el rasma deh is enough
2. modular arith.. page 101 geh bta3 el minus bayen(mesh sure)
3. gcd.. page 107, w el algo page 108 aw el algo el tanny page 111...aw el 2 bgad mesh fakra 7'ales bas wa7ed menhom aw el 2 gomm

Lost Security Exams:

1. Field, integral Domain, Commutative Ring, Abelian Group (Diagram),..

Questions + Sol:

1. Multiply 01010111 by 10000011 in GF(28) modulo m(x)=x8+x4+x3+x+1

Exam Qs Compilation:

1. Multiplicative inverse using extended Euc. alg.
2. Group, Ring , Field
3. two binary numbers multiply them in GF(2^3) , m(x)= X^3 +X +1 mod(29), GF(2^6), GF(2^8), mod(16) which of them can be used to encode binary data, which can be used but will increase the number of bits, which can't be used and why?
4. For each of the following equations, find an integer
5. that satisfies the equation. a. b. C. 9x K 8 (mod 7) 7x K 6 (mod 5) 5x K 4 (mod 3) X
6. Multiply 01010111 by 10000011 in GF(28) modulo m(x)=x8+x4+x3+x+1

Chapter 6: Block Cipher Operation

2010 Credit:

1. Modes of DES
2. Avalanche effect?

2021:

1. Draw OFB diagram.
2. Mentioned modes of operation of DES.
3. Which 2 encryption modes permit the block cipher encryption function to be called before the data is available?

2021 Extended:

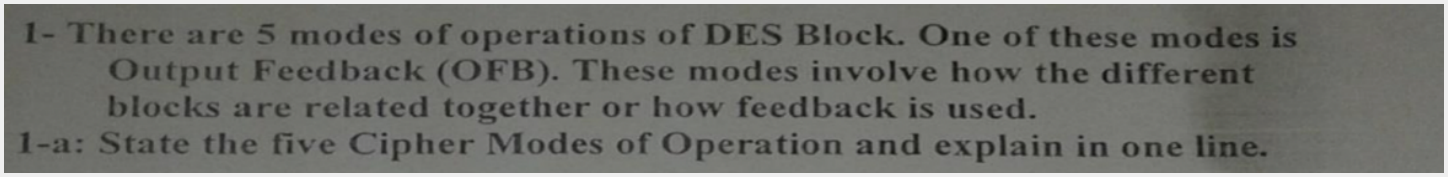
1. Mention modes of operation of DES (cbc, cfb,ctr,ecb,ofb)
2. Draw OFB diagram.
3. MCQ:
    a. Which block cipher mode is used for short data ECB
    b. DES round: key size=? input size=?
    c. Number of S-boxes
4. T/F:
    a. Some block cipher modes can be used to generate stream ciphers?
5. Write the term to which this definition refers:
    a. Two block cipher modes allow the block cipher encryption function to be called before the data is available? OFB & CTR

2017:

5 modes + diagram of OFB + OFB adv & disadv

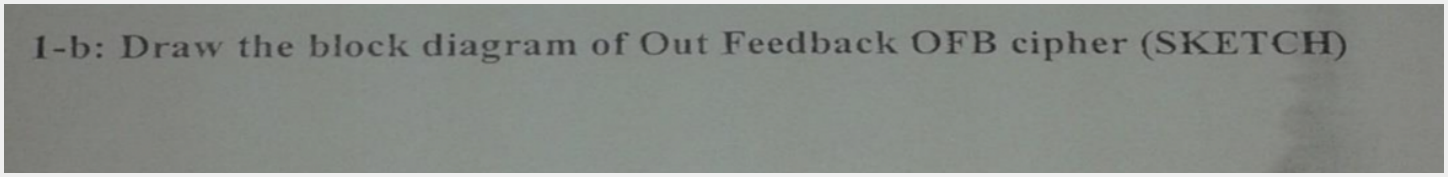
Is it possible to perform parallel block encryption using CBC mode , what about decryption?

2015:

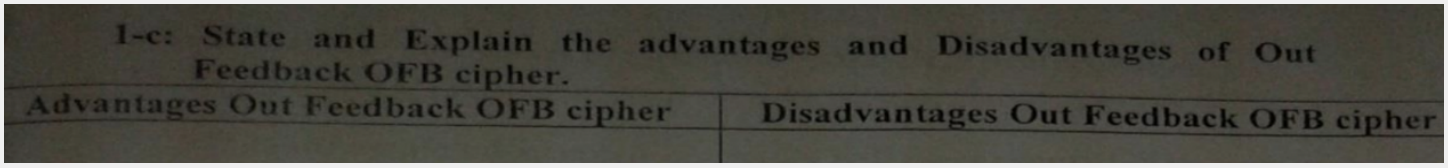


1- There are 5 modes of operations of DES Block. One of these modes is Output Feedback (OFB). These modes involve how the different blocks are related together or how feedback is used.

1-a: State the five Cipher Modes of Operation and explain in one line.

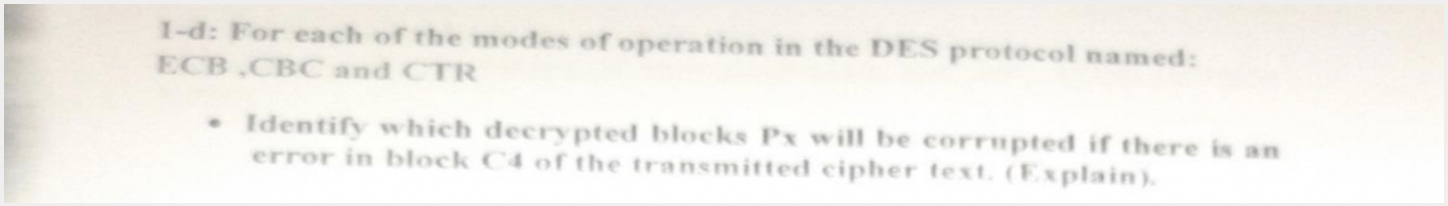


1-b: Draw the block diagram of Out Feedback OFB cipher (SKETCH)



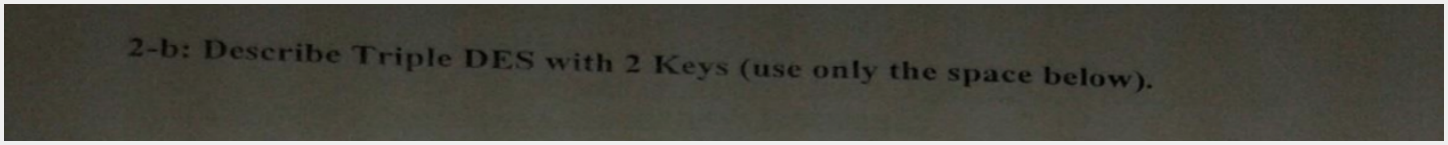
1-c: State and Explain the advantages and Disadvantages of Out Feedback OFB cipher.

Advantages Out Feedback OFB cipher	Disadvantages Out Feedback OFB cipher

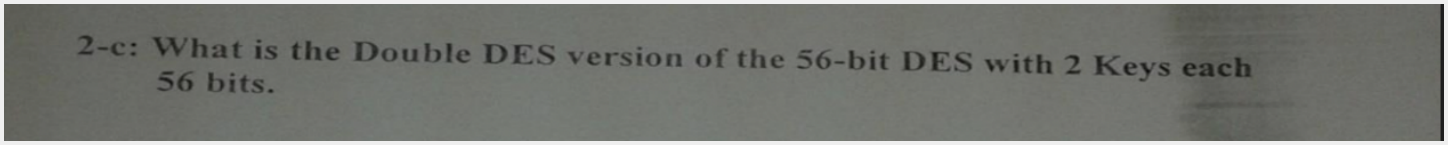


1-d: For each of the modes of operation in the DES protocol named: ECB ,CBC and CTR

- Identify which decrypted blocks Px will be corrupted if there is an error in block C4 of the transmitted cipher text. (Explain).



2-b: Describe Triple DES with 2 Keys (use only the space below).



2-c: What is the Double DES version of the 56-bit DES with 2 Keys each 56 bits.

2-d: Explain why Double DES with 2 Keys each 56 bits is much less secure than a single 112-bit DES? (Explain in detail and use sketch when possible).

5-b: About how many times more does a brute force key search take against a 112-bit DES than against a 56-bit DES?

2014:

1. Mention the Five modes of operation of Block Cipher?
2. Sketch the Output Feed Back Mode diagram and write the necessary equations for encryption and decryption?
3. Compare between OFB Advantages and Disadvantages?
4. Explain the Double DES and Triple DES and write the needed Equation for them? Draw the block diagram of both?
5. Why Double Des with two keys each one with size of 56 bits is less secure than Des with one Key with size of 112 bits?

2010:

1. State Block Cipher modes of operation. Choose one and discuss it.

2010-2:

1. Write the block cippher modes (EBC, CTR, C,,)
2. Draw the diagram for OFB

2010-Chapter:

1. Output Feedback (OFB) is one of the DES modes. List the other four modes.
2. Draw the block diagram of the OFB DES mode and illustrate it. Use symbolic forms in your illustration.
3. Why is it not good to encrypt two plain texts using the same key in stream ciphers?
4. Write the block cippher modes (EBC, CTR, C,,)
5. Draw the diagram for OFB

2010-Chapter:

1. Modes of DES
2. Avalanche effect?

Lost Security Exams:

1. ECB, CBC, CFB, OFB, Counter

Questions + Sol:

1. Output Feedback (OFB) is one of the DES modes. List the other four modes.
2. Draw the block diagram of the OFB DES mode and illustrate it. Use symbolic forms in your illustration.
3. (Final 2010) Why is it not good to encrypt two plain texts using the same key in stream ciphers?

Chapter 8: More Number Theory

Chapter 9: Public Key Cryptography & RSA

2010 Credit:

1. 6 requirements of public key
2. Draw Authentication and Secrecy

2021:

1. RSA Question.

2021 Extended:

1. Write RSA equations and prove them, then given p, q calculate private and public keys
2. RSA: if n=3599 and e=31 then d=?? (factorize n: 59*61)
3. RSA find ciphertext given e, p, q, plaintext

2017:

1. RSA algorithm + mas2la
2. RSA chosen cipher text attack (mas2la shabaho kda htt3ml b nafs el tare2a)

2014:

1. If RSA Algorithm were used and Bob and Alice where exchanging message, Bob leaks his Private key , and as a solution he decide to generate a new public and private key ? Is that safe? Illustrate your answer?

2010:

1. How to insure security and authentication using private and public key*

2010-2:

1. Securece & Authentication (A encrypts with PUb, PRa)
2. 6 requirements of public key

2010-Chapter:

1. Draw the public-key cryptosystem that provides both authentication and secrecy. Illustrate it.
2. Securece & Authentication (A encrypts with PUb, PRa) ...
3. 6 requirements of public key

2010-Credit*:-

1. Draw Authentication and Secrecy**
2. 6 requirements of public key

2007:

1. gat mas2ala f section 9.2 page 268
2. geh el RSA algo, el figure elly f page 270
3. ana kont katabt el algo elly f page 272 fel figure bas mesh fakra kan matlob wala et3'azt 3ashan kont fahmah f katabtoo
4. el toro2 to attack RSA, page 275 ettalabo nektebhom in brief

Lost Security Exams:

1. Requirements of public Key Encryption
2. Authentication and Secrecy
3. RSA
4. Security of RSA

Questions + Sol:

1. Draw the public-key cryptosystem that provides both authentication and secrecy. Illustrate it.
2. Compare between Conventional and Public-Key Encryption

Chapter 10: Other Public-Key Cryptosystems

2010 Credit:

1. Deffie Hellman(given q and a get x(a) 7aga zy kda)

2021:

1. Diffie-Hellman methodology and derivation.
2. Diffie-Hellman problem with q=71 and alpha= 7
    a. Xa=5 Xb=12 calculate Ya and Yb
    b. زي مسألة فاينال 2015 بنفس االرقام

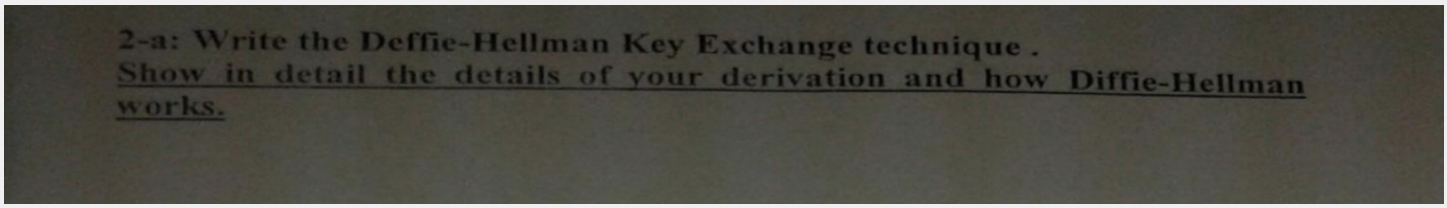
2021 Extended:

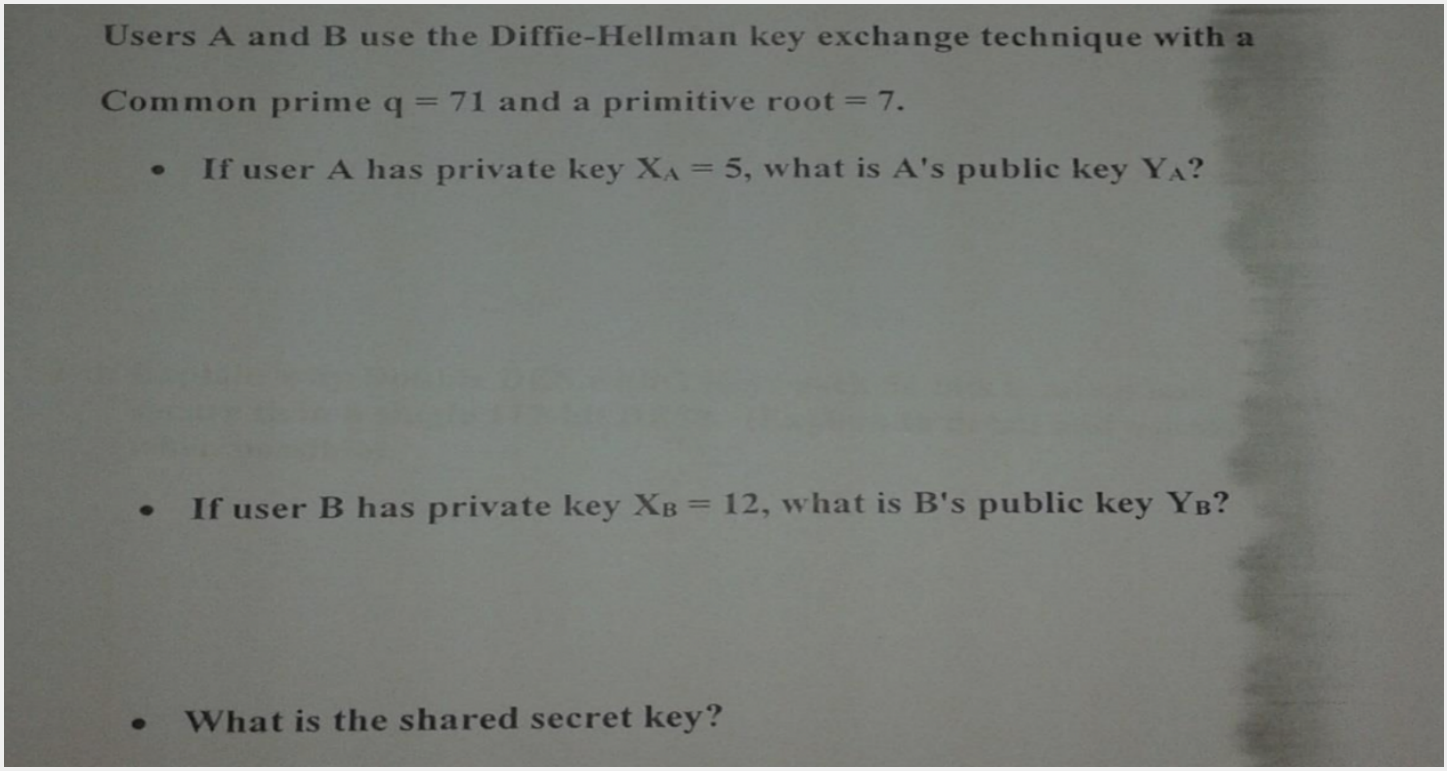
1. Write Diffie-Hellman's algorithm .
2. Deffie-Helman suffers from man-in-the-middle attack, explain.
3. Diffie-Hellman given q=71 and alpha= 7 , Xa=5 Xb=12 calculate Ya and Yb
4. MCQ Deffie- hellman

2017:

1. DH algorithm + mas2la + man in the middle attack + is it possible to perform man in the middle attack with just one key.

2015:





2014:

1. Write Equation of Diffie Hellman Algorithm and solve the following question ?
2. Given Q, A, XA calculate YA?
3. Given Q, A, XB calculate YB?
4. Calculate the shared Key KAB?

2010:

1. Diffie Hellman steps. (also a problem on it)

2010-2:

1. Deffie Hellman Algorithm , when it is used and a problem on it

2010-Chapter:

1. How Diffe-Hellman Works? Show the derivation. What is it used for?
2. Two users are using Diffe-Hellman with alpha = 7 and q = 71. If Xa = 5, compute Ya. If Xb = 12, compute
3. Yb. Compute the secret key. (this question is identical to problem 10.1 in the book)
4. Deffie Hellman Algorithm , when it is used and a problem on
5. it

2010-Credit*:

1. Deffie Hellman(given q and a get x(a) 7aga zy kda)

2007:

1. ta2reban compute the private key given the public key and an "easy-to-factor" n
2. Perhaps old book and this is Ch. 14:
    a. el 4 points bto3 page 291
    b. geh rasmeten men 4... el rosomat zay bta3et page 293 bas ana mesh fakra anhy
    c. menhom geh, bas as i think bta3et el public key page 293, certificate page 294

Lost Security Exams:

1. Diffie-Hellman
2. Elgamal
3. Diffie Hellman Man in the Middle

Questions + Sol:

1. How Diffe-Hellman Works? Show the derivation. What is it used for?
2. Two users are using Diffe-Hellman with alpha = 7 and q = 71. If Xa = 5, compute Ya. If Xb = 12, compute Yb. Compute the secret key. (this question is identical to problem 10.1 in the book)

Exam Qs Compilation:

1. RSA p,q key pair generation and encryption/decryption technique

Chapter 11: Cryptographic Hash Functions

2010 Credit:

1. Requirements of strong hash fn.

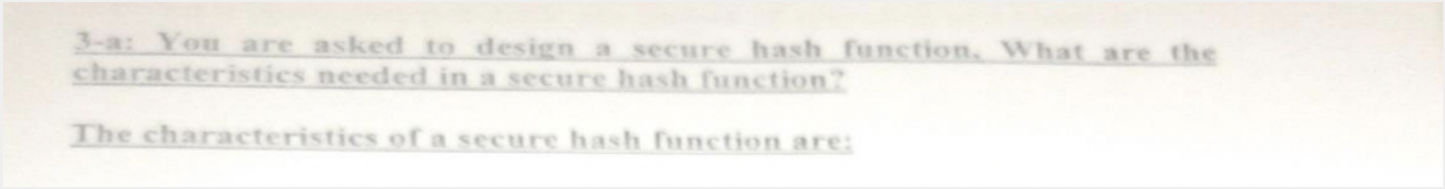
2021 Extended:

1. Since hashing generates a text that is not readable it can provide Confidentiality?

2017:

1. hash function requirements

2015:


3-a: You are asked to design a secure hash function. What are the characteristics needed in a secure hash function?

The characteristics of a secure hash function are:

2014:

1. what are the characteristics needed in secure hash function?

2010-2:

1. Requirements of strong hash fn.
2. compare between weak collision and strong collision?

2010-Chapter:

1. What are the three ways to do authentication?
2. What are the requirements for a strong hash function?
3. What is the difference between the weak collision resistance and the strong collision resistance?
4. Requirements of strong hash fn.
5. compare between weak collision and strong collision?

2010-Credit*:

1. Requirements of strong hash fn.

Lost Security Exams:

1. Requirements of strong hash function

Questions + Sol:

1. What are the three ways to do authentication?
2. What are the requirements for a strong hash function? (I think this question is so important)
3. What is the difference between the weak collision resistance and the strong collision resistance?

Exam I:

1. ch11...requirments of hash function
2. strong & week collision resistance

Chapter 12: Message Authentication Codes

2010 Credit:

1. Attacks that can be handled with MAC
2. 3 ways to do MAC

2021:

1. HMAC: design goals, what is the overhead over just using a hash function, diagram

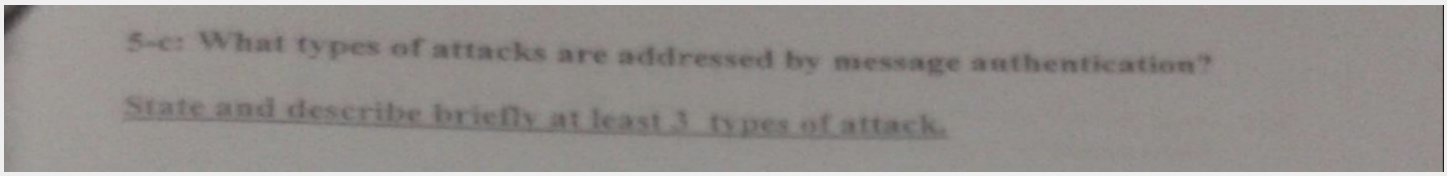
2021 Extended:

1. HMAC: design objectives, what is the overhead over just using a hash function , diagram
2. Draw HMAC block diagram and write all equations on it.
3. MAC can be used to provide both confidentiality and integrity?

2017:

1. all message attacks + brief description of each attack and how to handle each one
2. objective of HMAC
3. draw HMAC

2015:


5-c: What types of attacks are addressed by message authentication?

State and describe briefly at least 3 types of attack.

2014:

1. Mention 3 objective of the HMAC Design?
2. what types of attack are addressed by message authentication?

2010:

1. Message Authintication techiniques
2. Message authintication attacks

2010-2:

1. 3 ways to do MAC
2. Attacks that ccan be handled with MAC

2010-Chapter:

1. 3 ways to do MAC
2. Attacks that ccan be handled with MAC

2010-Credit*:

1. Attacks that ccan be handled with MAC
2. 3 ways to do MAC

Lost Security Exams:

1. Message Authentication Requirements:
2. Ways of achieving message authentication
3. HMAC Design Objectives
4. HMAC algorithm

Exam I:

1. ch12...message authentication tech
2. MAC requirements

Chapter 13: Digital Signatures

2021 Extended:

1. Digital signature is used for: verifying sender identity, in court ,prevent denial,all

Chapter 14: Key Management & Distribution

2010 Credit:

1. Draw Public Key Distr. (Authority or certificate)

2021:

1. Certificate requirements.
2. Content of certificate.
3. How can two parties share a session key without having public keys (diagram).
4. Write the term to which this definition refers:
    a. Document that validates public key?

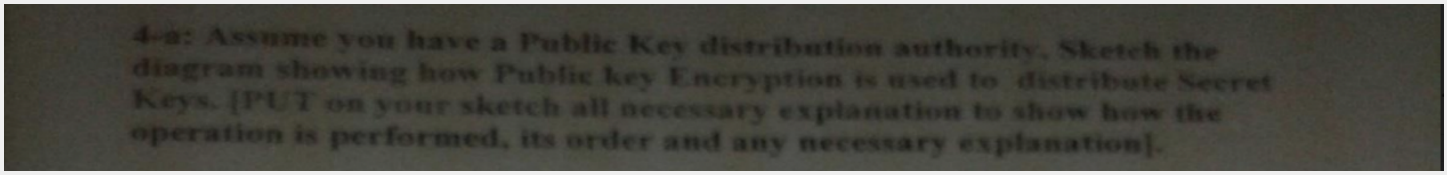
2021 Extended:

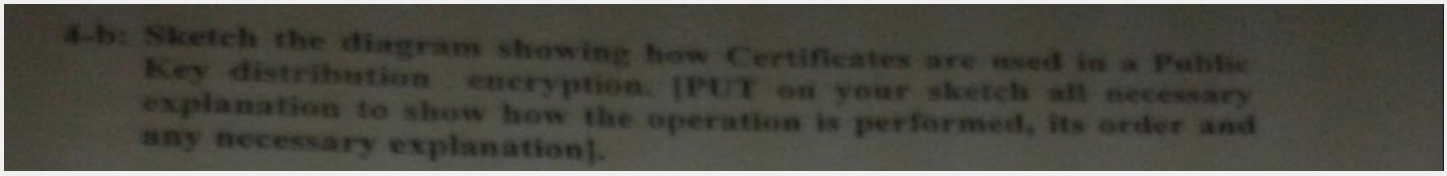
1. Certificate requirements.
2. Content of certificate.
3. How can two parties share a session key without having public keys (diagram).
4. Document that validates public key?

2017:

1. diagram public key encryption to distribute symmetric secret key
2. diagram of public key certificate
3. public key certificate requirements

2015:





2014:

1. What is the shared Secret Key?
2. Draw Authority Key Distribution mechanism and illustrate all the equations needed?
3. Draw Certificate Key Distribution mechanism and illustrate all the equations needed?

2010-2:

1. Pubic Key distribution using Authority

2010-Chapter:

1. Draw the public-key distribution scenario. Illustrate it.
2. Public Key distribution using Authority

2010-Credit*:

1. Draw Public Key Distr. (Authority or certificate)

2007:

1. Key distribution scenarios
2. compare link and end to end encryption page 205

Lost Security Exams:

1. Key distribution 6 diagrams

Questions + Sol:

1. Compare Link Encryption to End-to-End Encryption, and which do you think is more secure and why?
2. Draw the public-key distribution scenario. Illustrate it.

Exam Qs Compilation:

1. p.203 Compare between link encryption and end to end encryption
2. p.213 state the key distribution scenario
3. Compare Link Encryption to End-to-End Encryption, and which do you think is more secure and why?

Exam I:

1. ch7...link encryption & end to end encryption

Chapter 15: User Authentication Protocols

2021:

1. Write Needham equations. What is an obvious attack against it? How to counter it?
2. Needham suffers from man-in-the-middle attack, explain.

2021 Extended:

1. Write Needham equations. What is an obvious attack against it? How to counter it?

2017:

1. equations of Needham

2014:

1. Draw Needham Schroeder Protocol (KDC) , write equation and specify all the details of it ?
2. If we tried to use the Needham Schroeder Protocol in the E-mail Application , what the modifications to be done on it?

Lost Security Exams:

1. Needham and Schroeder Equations
2. Denning Equations

Chapter 16: Transport-level Security

2010 Credit:

1. Difference between SSL session and SSL connection
2. SSL participants (short statement on each) and the set

2021:

1. SSL Stack Diagram.
2. SSL Record Protocol operations and their security service.

2021 Extended:

1. SSL protocol stack Diagram.
2. SSL Record Protocol operations and their security service.
3. Difference between SSL session and SSL connection

2017:

1. ssl record protocol eh hwa
2. one field in ssl record protocol header
3. draw ssl architecture
4. choose 2 components of ssl architecture and write brief description
5. https consists of .... and ....
6. ssl alert protocol by3ml eh

2010:

1. SET diagram and scenario steps
2. Difference between Session and Connection.

2010-2:

1. SSL session & SSL connection
2. SET diagram and scenario steps
3. a large table related to SSL taking about each attach and how to overcome it , (copy paste from book)

2010-Chapter:

1. What is the difference between SSL session and SSL connection?
2. What are the SSL features that prevent the following attacks?
3. Note: there was a huge table consists of maybe 6 rows. There is an attack in each row (e.g. replay
4. attack) and you have to write the SSL features that prevent it.
5. SSL session & SSL connection
6. SET diagram and scenario steps
7. a large table related to SSL taking about each attach and how to overcom it , (copy paste from book)

2010-Credit*:

1. Difference between SSL session and SSL connection
2. SSL participants (short statement on each) and the set

2007:

1. el session key page 214

Exam Qs Compilation:

1. Difference between SSL session and SSL connection
2.
3. SSL features that prevent the following attacks
    a. Brute Force Cryptanalytic Attack: to 168 bits.
    b. Known Plaintext Dictionary Attack:
    c. Replay Attack:
    d. Man-in-the-Middle Attack:
    e. Password Sniffing
    f. IP Spoofing:
    g. IP Hijacking
    h. SYN Flooding

Chapter 20: Intruders

2021:

1. What is an Audit record? Why is it used?
2. What is a Honeypot? How is it used?
3. Types of intruders and their descriptions.
4. Mention the two techniques for detecting intruders and their description.

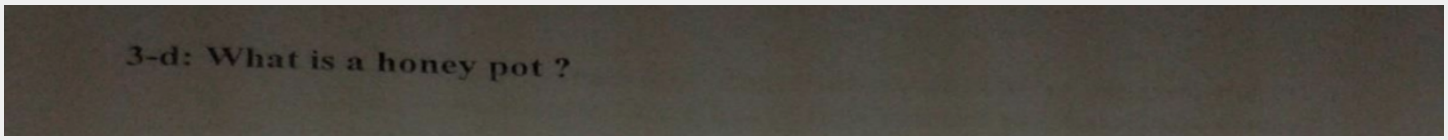
2021 Extended:

1. Types of intruders and their descriptions.
2. What is an Audit record? Why is it used?
3. What is a Honeypot? How is it used?
4. Mention the two techniques for detecting intruders and their description.

2017:

1. 3 classes of intruders
2. honeypot

2015:



2014:

1. Identify Classes of intruders?
2. What the common two technique to protect password file?
3. In intruder detection, what is the difference between statistical anomaly and rule based detection?
4. What is HoneyPot?
5. What is a salt in UNIX Password management and why is it used?
6. List 4 techniques to avoid guessable password?

2010:

1. What is SALT?

2010-2:

1. What is SALT in UNIX password managment?
2. 2 different ways to keep a password file secure(I guess)?
3. 4 methods to get passwords that are not gessable

2010-Chapter:

1. What is Salt? What is it used for?
2. What are the two ways to protect passwords?

3. What are the four ways to eliminate guessable passwords? Tell a statement about each.
4. What is SALT in UNIX password managment?
5. 2 different ways to keep a password file secure(I guess)?
6. 4 methods to get passwords that are not gessable

Lost Security Exams:

1. Types of intruders
2. Difference Between rule based intrusion detection and statistical intrusion detection
3. Password Scheme used in UNIX CRYPT(3)
4. Protection of password files
5. Password selection strategies

Exam I:

1. ch20...tech.to protect password file
2. statistical anomaly detection
3. rule based detection
4. SALT
5. tech. to avoid gussable password

Chapter 21: Malicious Software

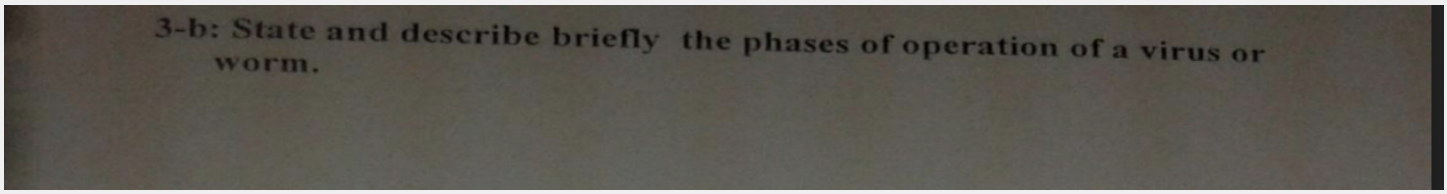
2021:

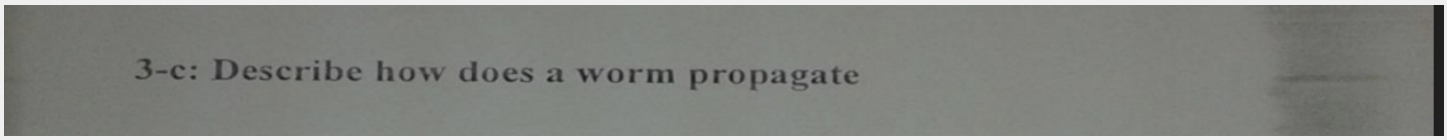
1. Types of malicious software, their description, and whether or not they need a host.

2021 Extended:

1. Types of malicious software, their description, and whether or not they need a host.

2015:





1. Worm and Virus lifecycle. Worm propagation lifecycle.
    a. The life cycle of Virus & Worms
    b. the propagation of worms

2014:

1. list and describe the 4 phases of operation of virus and worms?
2. describe how does the worm propagate?

1. 2010-Chapter:
2. What are the four phases of viruses and worms?
3. What are the functions performed by the propagation phase of a worm?
4. a-The life cycle of Virus & Worms
5. b-the propagation of worms

Questions + Sol:

1. Phases of worms and viruses
2. Difference between worm and virus
3. What are the functions performed by the propagation phase of a worm?

Exam I:

1. ch21...lifetime of virus and worms
2. propagation phase of worms
3. diff. bet. virus and worms

Chapter 21 Questions (NOP):

1. What is the rule of compression in the operation of the virus?
2. What is the rule of encryption in the operation of the virus?
3. What are typical phases of operation of virus or worm?
4. How does worm propagate?
5. What is a digital immune system?
6. How does behavior- blocking software work?
7. What is the DDos?

Other Chapters/Unknown

2010 Credit:

1. Problem on firewall to allow some addresses (fill a table of rules)

2010:

1. -Tunnel Mode and Transport Mode functionality- ---> Table p.493
2. -ipsec services?
3. - Firewall configuration problem (given some IPs with description, which ones to allow or deny for some services?)

2010-2:

1. A problem on firewall ,it looks similar to the table in the book
2. (src ,dst ,port , allow or disallow)

2010-Chapter:

1. What are the SET participants? Draw the figure of them. How does it work?
2. Fill a packet-filtering rules table given the explained rules in English.

Alice thinks that she has invented a protocol that makes her authenticate her peer (i.e. making sure that
it's Bob who is talking to her). The protocol proceeds as follows:
1- Alice generates a pseudorandom number

2- Alice encrypts this number with a previously shared key with Bob (i.e. assume no one knows the key
except Alice and Bob)
3- Alice sends the cipher text
4- Bob receives the cipher text
5- Bob decrypts the cipher text using the same shared key
6- Bob encrypts the output of step (5) using the same encryption key
7- Bob sends the output of step (6) to Alice
8- Alice receives this then decrypts using the same shared key
9- If Alice found the output of (8) the same number generated in (1), then It's true that Bob is the peer
of Alice. Else, it's not Bob who is communicating with Alice.
The question is: Is there an error in this protocol and if there is can you modify it to fix this error?

A problem on firewall ,it looks similar to the table in the book (src ,dst ,port , allow or disallow)

2010-Credit*:

1. Problem on firewall to allow some addresses (fill a table of rules)

2010 Concept:

CONCEPT QUESTIONS
*** Alice thinks that she has invented a protocol that makes her authenticate her

peer (i.e. making sure that it's Bob who is talking to her). The protocol proceeds
as follows
1- Alice generates a pseudorandom number
2- Alice ecrypts this number with a previously shared key with Bob (i.e. assume no
one knows the key except Alice and Bob)
3- Alice sends the ciphertext
4- Bob receives the ciphertext
5- Bob decrypts the ciphertext using the same shared key
6- Bob encrypts the output of step (5) using the same encryption key
7- Bob sends the output of step (6) to Alice
8- Alice receives this then decrypts using the same shared key
9- If Alice found the output of (8) the same number generated in (1), then It's
true that Bob is the peer of Alice. Else, It's not Bob who is communicating with
Alice.
The question is :D Is there an error in this protocol and if ther is can you modify
it to fix this error?

2007:

1. random no generator page 218 ma3a eno kan mal3'y:S:S

Exam I:

1. ch22...firewall problem configuration (hatla2eh table kber kda)