Started on	Tuesday, December 29, 2020, 8:00 AM
State	Finished
Completed on	Tuesday, December 29, 2020, 8:59 AM
Time taken	58 mins 36 secs

Question 1

Complete Marked out of 1.00

Given a DSA (digital signature algorithm) CryptoSystem with missing functional blocks:

At the sending side:

The Plaintext M is fed through a □ algorithm, output is then encrypted with

sender's private key

receiver's public key the Plaintext M.

At the receiving side:

M is fed through a □ algorithm, output is then decrypted with sender public key

to get D.

D is then compared with SHA-1 the receiving plaintext M send

Fill in the blank with correct choices

SHA-1

sender's private key

AES-256

receiver's private key

Question 2

Complete Marked out of 1.00

Which of the followings belong to Cryptography primitives ?

Select one or more:

□ Key exchange

□ Encryption Đ

□ Message authentication code Đ

☑ Hash Đ ✓

digital signature

Question 3

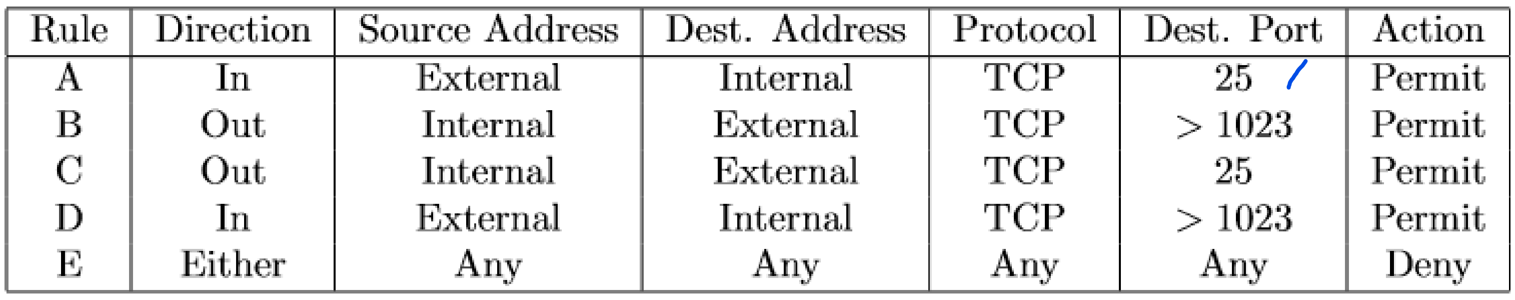
Complete Marked out of 1.00

Given a simple Packet-Filtering Firewall network layout:

Internal Network -----| Firewall |----- External Network

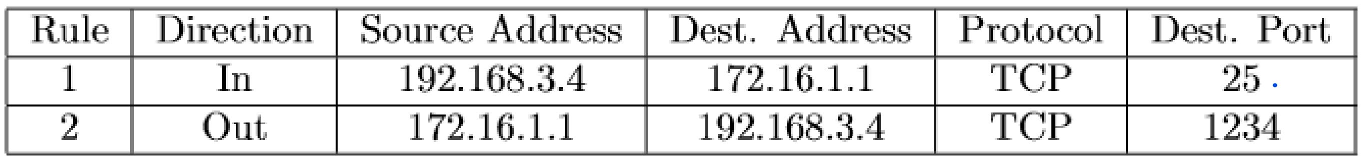
(172.16.1.0/24) (192.168.3.0/24)

The rules defined on firewall are given in the following table



Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
A	In	External	Internal	TCP	25 ✓	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

A computer on the External network (IP=192.168.3.4) sent a SMTP message to the mail server on the Internal network (IP=172.16.1.1). The rules for this communication can be described as:



Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port
1	In	192.168.3.4	172.16.1.1	TCP	25 .
2	Out	172.16.1.1	192.168.3.4	TCP	1234

Select the action of firewall for these packets and which rule of the firewall these actions are matched:

Rule	FW rule	FW Action
1	A ✓	Permit
2	B	Permit

Question 4

Complete Marked out of 1.00

What is the heart of a hashing function?

Select one:

○ a complex combination spliting then merging input

○ confusing then diffusing input

● a mathematical function that operates on 2 fixed-size blocks of data Đ ✓

○ a XORing function to operate on two inputs

Question 5

Complete Marked out of 1.00

In DES, the encrypting process of each round is actually:

Select one:

- ● S-Box function
- ○ a stream cipher
- ○ an MD5 algorithm
- ○ a Feistel function Đ

Since DES is based on the Feistel Cipher, all that is required to specify DES is

Round function
Key schedule
Any additional processing Initial and final permutation

Question 6

Complete Marked out of 1.00

Identify correct matches for the requirements of Cryptographic hash

Can not find 2 inputs that hash to the same output	strong	one-way resistance
No feasible way to modify a message without changing its hash value	week	Strong collision resistance
infeasible to invert the hash to get the source message	one way	Weak collision resistance

Question 7

Complete Marked out of 1.00

What is a Trojan horse could be?

Select one:

- ● It is a malicious software that allows other programs to control your computer by misleading users of its true intent Đ ✓
- ○ It is a computer virus that frequently attack computers
- ○ None of the choices is correct
- ○ It is a malfunction of the software that makes it difficult to navigate the Internet

Question 8

Complete Marked out of 1.00

Public-key Ciphersystem is vulnerable to:

Select one or more:

- □ Duplicate public-key
- ☑ Man in the middle attack (MITM) Đ ✓
- □ Tampered public-key
- □ Private key is duplicated

Question 9

Complete Marked out of 1.00

What are the Block Cipher primitives?

Select one or more:

- □ Diffusion Đ
- □ S-Box
- □ Confusion Đ ✓
- ☑ Multiple Round

Question 10

Complete Marked out of 1.00 1. false accpent rate or false positive rate

The percentage of times an invalid user is accepted by the system is called: [False positive rate] or [ ]

the percentage of times a valid user is rejected by the system is called: [ ] or [False negative rate]

reject rate or false negative rate

✓

Question 11

Complete Marked out of 1.00

How do the viruses infect programs?

Select one or more:

- □ insert themselves to the beginning of the infected programs Đ ✓
- □ the only way to infect is attaching themselves to the end of programs
- □ append themselves to the end of the infected programs Đ ✓
- ☑ embedded themselves in any portion of the infected programs Đ

Question 12

Complete Marked out of 1.00

You are a ‘very heavy’ user of mobile apps. You have apps that you use in your leisure time for staying informed about what happens in your city. You have apps that you use to keep in touch with your friends. Whenever you see an interesting app you want it and your instinct is just to download and install it.

However, for ensuring your safety and security it is best to…

Select one:

- ● Check that the app comes from a reputable source Đ ✓
- ○ Make sure you do not incur hidden costs when downloading an app
- ○ None of the choices is correct
- ○ Avoid having too many apps installed.

Question 13

Complete Marked out of 1.00

Check all statements that are true

Select one or more:

- ☑ Each operation or stage in AES is reversible Đ ✓
- ☑ To decrypt AES message, just run the same algorithm in the same order of operations.
- ☑ AES is much more efficient than Triple DES Đ
- ☐ AES can support key length of 128, 192, 256 Đ ✓

AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

Question 14

Complete Marked out of 1.00

Given a cipher algorithm:

Alice and Bob agree on the keyword K=(k1,k2,...,kt).
If t<n where n=|m|(the length of the message m) then they repeat the keyword until t=n

Encryption:
Alice uses the key ki to compute the ciphertext ci=(mi+ki) mod 26 for i=1,2,...,n

Alice then sends the ciphertext c=(c1,c2,...,cn) to Bob.

Decryption:

Bob uses the key ki to decrypt the ciphertexts mi=(ci−ki) mod 26 for i=1,2,...n

Choose correct name for the above cipher

Select one:

- ○ Affine
- ● Vigenére Đ ✓
- ○ Caesar
- ○ One-time pad

Question 15

Complete Marked out of 1.00

What weaknesses can be exploited in the Vigenere Cipher?

Select one or more:

□ It uses a repeating key letter

☑ It requires security for the key, not the message Đ ✓

□ The length of the key can be determined using frequency Đ ✓

Question 16

Complete Marked out of 1.00

Which of the following agents might defeat the rules imposing by the firewall?

Select one or more:

□ restricted softwares Đ

☑ restricted hardwares Đ ✓

☑ Mobile employee Đ

□ Laptop or other mobile devices

Question 17

Complete Marked out of 1.00

Which of the following are correct with worms?

Select one or more:

□ infect only files on a local computer

□ an independent malicious program that does not require host program. ✓

☑ use network connection to spread from one computer to another. Đ ✓

☑ a dependent malicious program that requires host program. Đ ✗

Question 18

Complete Marked out of 1.00

Given a Asymmetric CryptoSystem with missing functional blocks:

At the sending side:

The Plaintext M is fed through a [ ] algorithm, output is then encrypted with [AES-256]

[ ] to get C.

[receiver's public key] the Plaintext M.

At the receiving side:

M is fed through a [ ] algorithm, output is then decrypted with [ ]

to get D.

D is then compared with C [SHA-1] the receiving plaintext M [receiv

Fill in the blank with correct choices

SHA-1

sender's private key

AES-256

receiver's public key

Question 19

Complete Marked out of 1.00

Three components of an IDS

Select one or more:

- □ Log
- ☑ Analyzer Đ
- ☑ Sensors Đ ✓
- ☑ Interface Đ

Question 20

Complete Marked out of 1.00

Which of the following belong to control techniques of firewall?

Select one or more:

- □ flag bit
- □ behavior Đ
- ☑ service Đ
- □ direction Đ ✓
- ☑ user Đ

Question 21

Complete Marked out of 1.00

In symmetric key encryption, how many keys are needed for a group of n people to communicate with each other?

Select one:

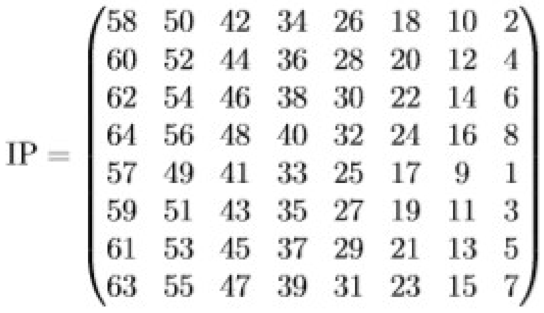
- ● n*(n-1)/2 Đ
- ○ n/2
- ○ n*(n-1)
- ○ log(n)

Question 22

Complete Marked out of 1.00

In DES encryption, there are 3 stages: (1) Initial permutation, (2) multiple-round of confusion and diffusion, (3) Final permutation

P-Box of (1) is given below:



$$\mathrm{IP} = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

Which of the followings are correct about this P-Box?

Select one or more:

- ☑ the 32nd bit of the output is taken from the 29th bit of the input
- □ the 8th bit of the output is taken from the 2nd bit of the input Đ
- □ the 1st bit of the output is taken from the 58th bit of the input Đ
- □ the 58th bit of the output is taken from the 1st bit of the input

Question 23

Complete Marked out of 1.00

Identifiy the cipher's name in the following algorithm:

Alice and Bob agree on the 56-bit key K

Encryption:

Alice uses the key K in the key schedule to generate the 16 48-bit round keys K1,K2,...,K16 then uses the round keys in the order K1,K2,...,K16 in an E algorithm to encrypt the message c=E(m).

Alice sends the 64-bit ciphertext c to Bob.

Decryption:

Bob uses the key K in the key schedule to generate the 16 48-bit round keys K1,K2,...,K16 then uses the round keys in the reverse order to decrypt the ciphertext c by m=D(c)

Select one:

● SHA-64

○ DES Đ

○ AES

○ AES-64

Step 1: Receives {m’ , Mac} (message denoted as m’ because its integrity is uncertain)
Step 2: Generate mac' =MAC(m' , k) from m' and k.
Step 3: Compare mac' with mac
Step 4: if mac=mac' then Bob knows the message has not changed in transit

Question 24

Complete Marked out of 1.00

Alice wants to send a message to Bob. Alice wants Bob to be able to verify that the message has not changed in transit. For this, they use a MAC function with a shared secret key k for generating and verifying a MAC value. Briefly, outline the cryptographic steps that Bob must follow to validate the integrity of the message after getting it from Alice.

Step 1: if mac=mac' then Bob knows the message has not changed in transit

Step 2: Generate mac'=MAC(m', k) from m' and k.

Step 3: Receives {m’, Mac} (message denoted as m’ because its integrity is uncertain)

Step 4: Compare mac' with mac

Question 25

Complete Marked out of 1.00

12

For access control in Unix file system, ~~2~~ protection bits are used

Question 26

Complete Marked out of 1.00

In terms of non-repudiation, which of the following primitives is provided?

Select one or more:

- ☑ Digital signatures + Public Key certificate Đ ✓
- □ Hash functions
- □ Digital signatures
- □ Encryption
- □ Message Authentication Codes (MAC)

Question 27

Complete Marked out of 1.00

In Diffie-Hellman Key Exchange, both parties choose a prime number (p) and a generator g which is a primitive root of p. What would happen if g is not a primitive root of p?

Select one or more:

- □ g^x mod p yields a set of unique value between 1 and p-1
- □ g^x mod p yields cyclic groups
- ☑ g^x mod p does not yield cyclic groups Đ
- ☑ The cipher is vulnerable Đ ✓

Question 28

Complete Marked out of 1.00

Identify bots and definitions

Used by botmasters to fraudulently increase revenue from advertisers Click

Used to gather valuable financial information Phishing

Infected machines send out emails spamming ✓

Spamming

Click fraud

Phishing

Question 29

Complete Marked out of 1.00

In terms of message integrity, which of the following primitives is provided?

Select one or more:

- □ Digital signatures Đ
- ☑ Hash functions Đ ✓
- □ Encryption
- □ Message Authentication Codes (MAC) Đ ✓

Question 30

Complete Marked out of 1.00

What are correct primitive roots of 17

Select one or more:

☑ a. 3,5,6,7,10,12,13,14

□ b. 2,3,5,11,13 Đ ✓

□ c. 2,7,9,11,14

□ d. 3,5,7,9

Question 31

Complete Marked out of 1.00

Which of the following does not belong to security services that cryptography provided?

Select one or more:

□ accountability Đ

□ Availability Đ

□ obscurity Đ

☑ Message authentication ✓

Question 32

Complete Marked out of 1.00

In an intrusion detection system, sensors are used to collect information about network usage. Which type of sensor can be used to block network traffic.

Select one or more:

□ None of the choices is correct

□ Passive

☑ Inline Đ ✓

□ Active

Question 33

Complete Marked out of 1.00

What is the collision resistance of SHA-256 hash function?

Select one:

○ 2^64

○ 2^128 Đ ✓

● 2^64

○ 2^256

Question 34

Complete Marked out of 1.00

What are available techniques for intrusion detect?

Select one or more:

☑ Anomaly detection Đ ✓

☐ Signature-based detection Đ ✓

☐ malware-based detection

☑ Rule-based detection Đ ✓

Question 35

Complete Marked out of 1.00

Which of the followings is preferred when attacker designs DNS-based Botnet C&C?

Select one:

○ Dynamic DNS Đ ✓

● Caching DNS

○ forward DNS

○ Static DNS

Question 36

Complete Marked out of 1.00

Which of the following are correct features of DES in terms of input block size, key length, and output block size (M,K,C)?

Where

M: Message,

K: Key

C: Encrypted message

Select one or more:

☐ M=128, K=56, C=65

☑ M=64, K=64 (including parity bits), C=64 Đ ✓

☐ M=64, K=56, C=64

☐ M=Arbitrary, K=64, C=56

Question 37

Complete Marked out of 1.00

Which of the following are true about MAC?

Select one or more:

- ☑ MAC is actually hash function Đ ✓
- □ MAC has fixed-length output while hash has variable length output Đ ✓
- □ MAC is a keyed hash function Đ ✓
- ☑ MAC can provide message authentication ✓

Question 38

Complete Marked out of 1.00

One day when looking at your e-mail inbox, you find you have received an email from a friend you have not heard from for at least one year.
When you open the email the text says '*Hi, please click here* http://shorturl.jhdsuyc.com, *there is a surprise for you*'.

What would you do in such scenario?

Select one:

- ○ Click on the link, since the sender (friend) of the e-mail is known
- ● None of the choices is correct
- ○ Click on the link only if it looks somehow familiar to you
- ○ Do nothing with the e-mail – and, certainly, don't click on the link Đ ✓

Question 39

Complete Marked out of 1.00

Which utility is that hackers often used to gather information about the target system?

Select one:

- ○ nmap Đ ✓
- ○ fullmap
- ● wireshark
- ○ sqlmap

Question 40

Complete Marked out of 1.00

Which of the following belong to security services that cryptography provided?

Select one or more:

- ☑ Privacy Đ
- ☐ Availability
- ☐ Message authentication Đ
- ☐ Integrity Đ

Question 41

Complete Marked out of 1.00

Which of the following are Cryptography primitives?

Select one or more:

- ☐ Hash functions Đ
- ☐ Message Authentication Codes (MAC) Đ
- ☑ Key-exchange
- ☑ Encryption Đ
- ☐ Digital signatures Đ
- ☑ password hashing

Question 42

Complete Marked out of 1.00

Select all the correct answers to complete that statement: A block cipher should...

Select one or more:

- ☑ use a few rounds, each with a combination of substitution and permutation. Đ
- ☐ Use permutation to achieve diffusion
- ☐ Keep the algorithm secret
- ☐ Use substitution to achieve confusion

Question 43

Complete Marked out of 1.00

Which of the following are used by a typical packet filtering firewall?

Select one or more:

☐ Time to live

☐ Internet Header Length

☑ Destination IP Đ

☑ Destination port Đ ✓

☑ Source IP Đ

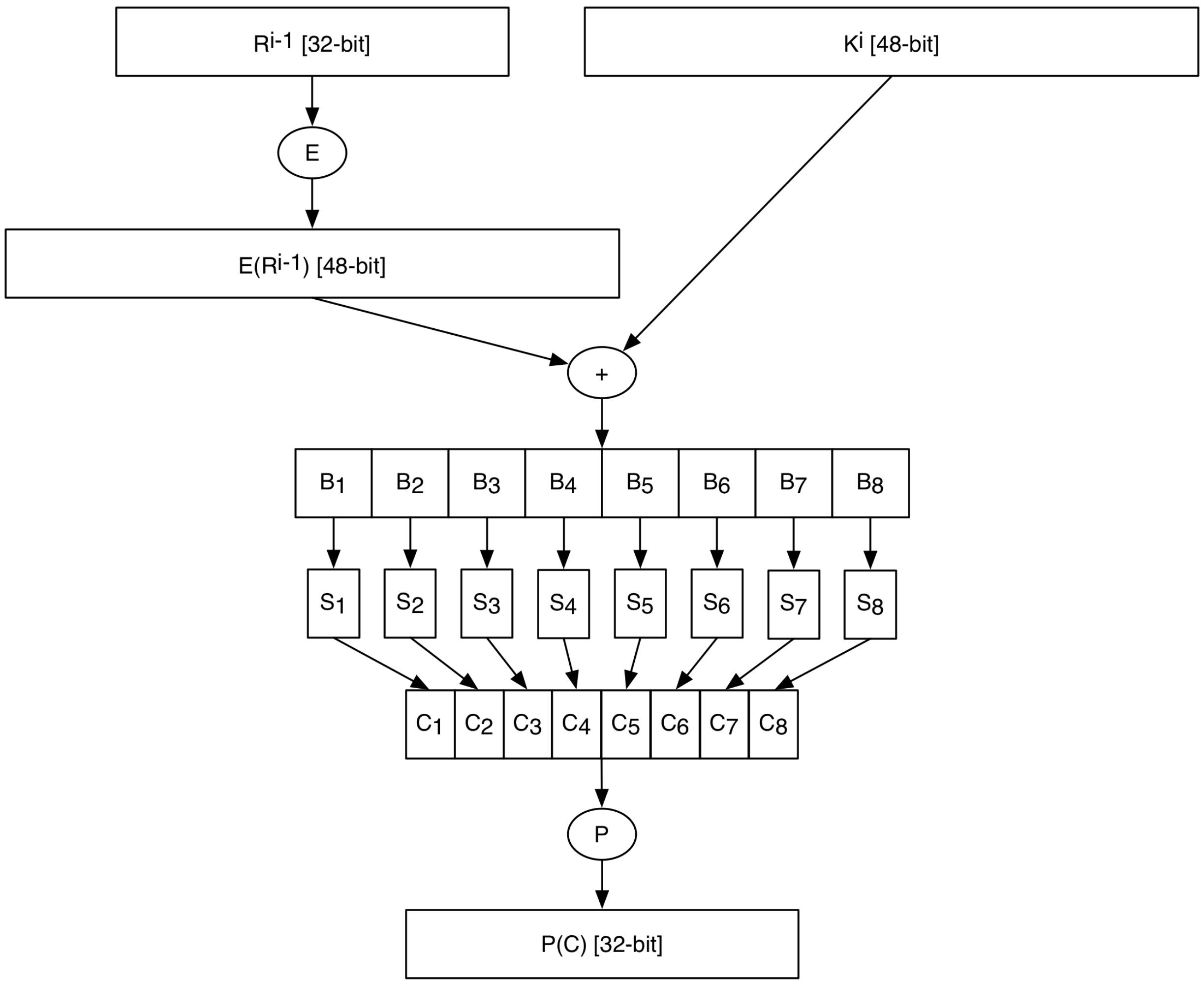
☑ Source port Đ

☐ Checksum

Question 44

Complete Marked out of 1.00

Identifiy the cipher's name in the following figure



R^{i-1} [32-bit]
K^i [48-bit]
E
$E(R^{i-1})$ [48-bit]
+
B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8
S_1 S_2 S_3 S_4 S_5 S_6 S_7 S_8
C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8
P
P(C) [32-bit]

Select one:

○ SHA

○ DES

● MD5 Đ ✓

○ Feistel

Question 45

Complete Marked out of 1.00

Check all tasks for which asymmetric encryption is better:

Select one or more:

- □ scalability
- ☑ provide confidentiality of a message Đ
- ☑ securely distribute a session key Đ

Question 46

Complete Marked out of 1.00

Which of the following does not belong to Cryptography primitives ?

Select one or more:

- □ DES Đ
- □ Digital signature
- □ Key exchange Đ
- ☑ Hash

Question 47

Complete Marked out of 1.00

Which of the following could be the weaknesses of the packet-filter firewall?

Select one or more:

- □ Attacks and exploits that take advantage of problems within the TCP/IP specification
- ☑ logging functionality in packet filter might easily take up space of firewall storage Đ
- □ Attacks that employ application-specific vulnerabilities or functions
- ☑ Easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy Đ

Question 48

Complete Marked out of 1.00

These days in the media it is not uncommon to hear that organizations and companies have suffered from cyber-attacks.

The popular image is that these attacks are carried out by so-called malicious hackers that are external to an organization. However several observations show that many of these attacks are carried out by organization employees/officers or former employees.

What is the common name which is given to this latter type of threat?

Select one:

● Ethical hacking

○ None of the choices is correct

○ Trolling

○ Insider Threat Đ ✓

◄ Submission for PKI lab

Jump to...

review123 ►