Page No.:

Date: 24/05/21

γουνλ

Mock Test

CSS

AMEY MAHENDRA THAKUR

TE COMPS B-50

TU3F1219127

22

Q2A) RSA n=221 & e=5 d=3

Q2A) Diffie-Hellman 9=7, P=23, x=3, y=5

B2B] Digital Certificate X.509 standard

Q3.

Q3A] ARP Spooting and Post Scanning

Q3B] Cross - site scripting (xss) with its types

esqyt 271 mico evril [88]

NAME: AMEY MAHENDRA THAKUR

COMPS TE B

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO .: 1/7

6(A)
RSA
n = 221 $e = 5$
There are two requirements
- n must be a product of two primes - e must be relatively prime to $\Phi(n)$.
- of rover be a prime to $\phi(n)$.
- 6 wat be reidilized
First requirement
n = 221 = 13.17 13 and 17 are primes
So this holds.
Second requirement
Second requirement If $n = p \cdot q$ where p and q are distinct Primes. then $p \cdot q = (p-1) \cdot (q-1)$ So, $p \cdot (221) = (13-1) \cdot (17-1) = 12 \cdot 16 = 192$
Drines then $O(p,q) = (p-1) \cdot (q-1)$
(12-1) = (13-1). (17-1) = 12.16 = 192
e # d mod b(n) =1 , 5 # d mod 192=1
E T d mod W(h)
1. Pallanda method
d is calculated using the following method
We continue get an interest
$d = \left[\phi(\eta)^* \right] + 1 = \left[\frac{1921}{5} \right]^{-38.6}$
e
where, 1 = 1 to 100
the second of th

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO.: 2/7

1-02 1=5
d = (192 × 2) +1
5
= 384 + 1
5
= 385
S
∴ d = 77

SIGNATURE: And

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO.: 3 /7

6 (A)
Diffie - Hellman Protocol
g = 7 $p = 23$ $x = 3$ $y = 5$
$R_1 = P^{\times} \mod g = 23^3 \mod 7$
= 12167 mod 7
$R_1 = 1$
R2 = Py mod q = 235 mod 7
= 6436343 mod 7
$R_2 = 4$
Secret ken 1 = R2 mod g
Secret key $1 = R_2 \mod q$ $= 4^3 \mod 7^0$
Secret Key 2 = Ris mod 9
= 15 mod 7
=
Secret key 1 = Secret key 2 = 1
Secret Koy.
: Sagnethmetnic Key & =)
- Style of the sty

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO.: 4/7

Q(B)
Digital Certificate ×.509 standard
J
- Digital certificate is an electronic file that is
used to identify people and resources over a
insecure channel or a network called internet.
Digital certificate also enable secure confidential
Communication between sender and megiver
using encryption.
- For example when we travel to another country
our passports provides a way to establish
Our identity and gain entry Digital certificate
Our passports provides a way to establish Our identity and gain entry Digital certificate provide similar identification in the electronic
-world.
- The role of Certification Authority (CA) is to
issue certificates with authorized ditital signature
Much like the role of the passport office.
the role of the CA is to ralidate the certificate
so that it cannot be tampered by
so that it cannot be tampered by
unauthorized user.
- Once a CA has signed a certificate the
Owner can present their certificate to people
web sites and network resources to prove
their identity for confidential communications over inserve channel
over inservé channel

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1 **PAGE NO.:** 5/7

A standard colled as X-509 define structure of digital certificate. The International Telecommunication Union (ITU) permitted this Standard in 1998. The following diagram shows the structure of X.509 digital certificate. Digital certificate Centents. Certificate Version Number Certificate Series Number Algorithm for signature identifier Certificate Issues Name Validity Details Name of the certificate Owner Public Key of Certificate Owner I scuer Unique Identifier Certificate Authority (M) Digital signature - Restandard digital certificate typically includes a variety of information pertaining to 113 Owner and to the Certificate Authority (A Treated Agency that can icsue Digital Certificate)	
Telecommunication Union (ITU) permitted this Standard in 1998. The following diagram shows the structure of X. 509 digital certificate Centents Certificate Vertical Number Certificate Serial Number Algorithm for signature identifier Certificate Issuett Name Validity Details Name of the certificate Owner Public Key of Certificate Owner I ssuer Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority (11) pigital signature Structure of X. 509 pigital Signature	- A standard called as X-509 defines structure
Standard in 1998. The following diagram shows the structure of X. 509 digital certificate. Digital certificate Centents. Certificate Version Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Keyn of Certificate Owner T saver Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X. 509 Digital Signature	or digital certificate. The Tota national
The following diagram shows the structure of X. 509 digital certificate. Digital certificate Centents Certificate Version Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public key of Certificate Owner Issuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X. 509 Digital Signature	Telecommunication Union (ITU) permitted this
The following diagram shows the structure of X. 509 digital certificate. Digital certificate centents Certificate Verticos Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public key of Certificate Owner I sever Unique Identifier Extentions to certificate Certificate Authority ((A) Digital signature Structure of X. 509 Digital Signature	Standard in 1998.
Digital Certificate Contents Certificate Vertion Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Key of Certificate Owner Issuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	
Digital Certificate Contents Certificate Vertion Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Key of Certificate Owner Issuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	The following diagram shows the structure of
Digital Certificate Contents Certificate Vertion Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Key of Certificate Owner Issuer Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	X. 509 digital certificate
Certificate Version Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name Of the certificate Owner Public Key of Certificate Owner I szuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital Signature Structure of X.509 Digital Signature	
Certificate Vertion Number Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name Of the certificate Owner Public Key of Certificate Owner I szuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital Signature Structure of X.509 Digital Signature	Digital Certificate Contents
Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Key of Certificate Owner Issuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	
Certificate Serial Number Algorithm for signature identifier Certificate Issuest Name Validity Details Name of the certificate Owner Public Key of Certificate Owner Issuer Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	Certificate version Number
Algorithm for signature identifier Certificate Issues Name Validity Details Name of the certificate Owner Public Key of Certificate Owner I sever Unique Identifier Owner Unique Identifier Extentions to certificate (extificate Authority (A) Digital signature Structure of X.509 Digital Signature	1
Certificate Issues Name Validity Details Name of the certificate Owner Public Key of Certificate Owner I sever Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	
Name of the certificate owner Public key of Certificate owner I sever Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X.509 Digital Signature	
Public Key of Certificate Dwarn I sever Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority ((A) Digital signature Structure of X.509 Digital Signature	
Public Key of Certificate Dwarn I sever Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority ((A) Digital signature Structure of X.509 Digital Signature	Name of the certificate owner
I sever Unique Identifier Owner Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X. 209 Digital Signature	
Owner Unique Identifier Extentions to certificate Certificate Authority (A) Digital signature Structure of X. 509 Digital Signature	
Extentions to certificate Certificate Authority (A) Digital signature Structure of X. 509 Digital Signature	
Structure of X. 209 Digital Signature	
Structure of X. 209 Digital Signature	
- A standard digital certificate typically included a variety of information pertaining to its owner and to the Certificate Anthority (A Trusted Agency that can issue Digital Certificate)	
a variety of information pertaining to the owner and to the Certificate Anthority (A Tryated Agency that can issue Digital Certificate)	- A standard digital certificate typically includes
Owner and to the Certificate Anthority (A Trusted Agency that can issue Digital Certificate)	a variety of information pertaining to its
(A Trusted Agency that can issue Digital Costificate)	and to the Certificate Anthority
	(A Tonated Agency that can issue Digital Costificate)

NAME: AMEY MAHENDRA THAKUR

COMPS TE B

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO.: 6/7

Such as:
1 Contificate Version Humber
- Identifies a particular version of the x. 509
Chorend version : 1 X.509 VB
2) Certificate Scotal Number
- Unique Integer Number generated by costition
aumority
3) Algorithm for signature Identifier.
- Identice algorithm used by the certification authority to sign the certificate
authority to sign the certificate
@ Certhicate Isover Name
- The name of the certification arthority
that isoved the contitleate
Indt 17000 Inc Continues
E) Validity Dubails
- The ralidity period of the certificate
6) Name of the certificate owner
- The name of the owner and where
- The name of the owner and where identification information required for
identifying the owner such as email IP and
identification information required too identifying the owner such as enail IP and confact details

ROLL NO.: 50

SUBJECT: CSS

EXAM: IAT-1

PAGE NO.: 7/7

@ Public key of cernficate owner
- Certificate owners public key which is used to encrypt confidential information of the certificate
encrypt confidential information of the certificate
Over
8 Issuer Unique Identifier
- Identify the CA uniquely
9 Duner Unique Identifier
- Identify the owner uniquely
V
@ Extentions to certificate
- This is an optional field which allows a
CA to add additional private information to
the certificate
(11) Certificate Authority (A) Digital Signature
- In creating the creatificate, the information is digitally signed by the issuing (A.
digitally signed by the issuing (A.
<i></i>