__/__/____

1. 3 core components of a PKI:

Digital certificates
- serves as digital identity for company/website
- used for verification while communicating
- certificates issued by certificate Authorities

Certificate Authority
- Authorized users/companies/websites
- Parties provide root trust for verification

Registration Authority
- They issue digital certificates for specific users permitted by a higher level certificate
- They maintain, or revoke authorized certificates
- store in an encrypted database

2. The four requirements for Kerberos are:
Authentication, confidentiality, Integrity, Single Sign On

3.

a. Symmetric Key Encrypted Session Key Packet
b. Modification Detection Code Packet
c. Signature Packet
d. Combo of signature + Modification Detection Packets
e. Combo of symmetrically Encrypted Data + Modification Detection
f. Combo of Symmetric Key Encrypted session key + signature
g. Combo of Symmetric Key Encrypted Session Key, Modification Detection Code and Signature Packets
h. Combo of Symmetric Key Encrypted Session Key, Modification Detection Code and Signature Packets.

__/__/____

4.

a. Encrypted Data

b. Signed Data

c. Signed Data

d. Signed Data

e. Signed + Encrypted Data

f. Signed + Encrypted Data

g. Signed + Encrypted Data

h. Signed + Encrypted Data

5. Digital Signature Attacks:

- Target - authenticity and integrity of message
- common attacks - forgery, message tampering, compromised key signage
- counters - secure private keys, strong cryptographic algorithms, using digital certificate infrastructure to authenticate public keys

Cryptosystem Attacks:

- Target - confidentiality of data
- common attacks - cryptanalysis, brute force, timing attacks
- counters - longer key sizes, secure key management, stronger cryptographic algorithms

6. Main features of SHA 512:

- 64 byte message
- 128 byte block size
- low collision
- 80 hash rounds
- compression function depends on previous output

The Davies-Meyer function is used in SHA 512

__/__/____

7. Birthday attacks take advantage of the birthday paradox, which states that two people selected randomly actually have a very high chance of sharing a birthday.

This attack tries to exploit collisions in a hash function to understand any secure keys and algorithms. An attacker will try multiple inputs to try and get a collission, allowing them to study the algorithms better.

8. Ch

a. The one way part of RSA is computing the value of n from two large primes p, q. This is one way due to the complexity of prime factorisation.

b. The trapdoor of RSA is performing a modular logarithm. Both encryption and decryption rely on modular exponentiation, requiring modular logarithms to crack a cipher, requiring knowledge of primitive roots of a large value.

c. The private key is the key the server ~~shares~~ maintains, the public key is a shared keys to clients. clients can encrypt messages with the public key, which can easily be decrypted using the private key at the server.

d. RSA is secure due to the impractical nature of brute forcing prime factorisation and modular arithmetic. But advances in quantum computing may crack prime factorisation.

__/__/____

9. $(\mathbb{Z}_4, +_7)$ table

$+_7$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

For abelian group : $a + b = b + a$

The operation table is equivalent to its transpose

∴ For every $a + b = b + a$

∴ $(\mathbb{Z}_4, +_7)$ is an abelian group

b. $3 + 2 = 5 \bmod 4 = 1$

$3 - 2 = 1 \bmod 4 = 1$

10.

- x
- $x + 1$
- x^2
- $x^2 + 1$

__/__/____

10. Assuming ($GF 12^3$)

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

X	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	011	001
011	000	011	110	101	011	000	111	100
100	000	100	101	011	110	010	001	111
101	000	101	111	000	010	101	111	010
110	000	110	011	111	001	111	101	010
111	000	111	001	100	111	010	010	101