2013

Question 2

a

Symmetric

- Uses one key
- Sender and receiver both access to the key
- Algorithms such as DES, AES
- Used to keep information private
- Much less costly, so can be bigger and thus more difficult to brute force
- Difficult to get the key to the other person whilst keeping it private

Asymmetric

- Key pairs
  - Public and private key
- Sender and receiver both have their own key pairs
  - Also have access to each others public keys
- Algorithms such as RSA, Diffie-Hellman
- Used for authentication, verification, and to distribute symmetric keys
- More costly to generate and use (more requirements), therefore smaller and easier to brute force

Can asymmetric cryptography to securely pass a symmetric key to another person

1. Alice generates key pair
2. Send Bob public key
3. Alice generates symmetric key
4. Signs with her private key and encrypts with her public key to send
5. Bob decrypts the message after verifying it's Alice
6. Alice and Bob can now use the symmetric key for encryption/decryption

b

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

```
THIS IS AN EXERCISE
MABL BL TG XQXKVBLX
```

- The shift can only be a number between 1 and 25
  - Small brute force space
- Common letters in the language can be identified
  - Example `E` is the most common letter in English
- Common words can be identified
  - `a`, `an`, `the`, `is`, etc.

c

- $e = 17$
- $n = 187 = 11 \times 17$
- $\phi(n) = (11 - 1)(17 - 1) = 160$

$$d \equiv e^{-1} \mod \phi(n)$$

- $d \equiv 17^{-1} \mod 160$
- $\gcd(160, 17) = 1$
  - $160 = 17 \times 9 + 7$
  - $17 = 7 \times 2 + 3$
  - $7 = 3 \times 2 + 1$
  - $3 = 1 \times 3 + 0$
- Back substitution
  - $1 = 7 - 3 \times 2$
  - $1 = 7 - 2 \times (17 - 7 \times 2)$
  - $1 = 7 + 4 \times 7 - 2 \times 17$
  - $1 = 5 \times 7 - 2 \times 17$
  - $1 = 5 \times (160 - 17 \times 9) - 2 \times 17$
  - $1 = 5 \times 160 - 45 \times 17 - 2 \times 17$
  - $1 = 5 \times 160 - 47 \times 17$
- $17^{-1} = -47$
- $d \equiv -47 \mod 160 \equiv 113$

d

Authentication Header

- Guarantees connectionless integrity and data origin authentication of IP packets

- It can optionally protect against replay attacks by using the sliding window technique and discarding old packets
- Operates directly on top of IP using IP protocol number 51

Encapsulation Security Payload

- Provides origin authenticity, integrity and confidentiality protect of packets
- Supports encryption-only and authentication-only configurations
  - Using encryption without authentication is strongly discouraged
- ESP in transport mode does not provide integrity and authentication for the entire IP packet
  - In Tunnel Mode, where the entire origin IP packet is encapsulated with the new packet header added, ESP protect is afforded to the whole inner IP packet

Question 3

d

	TCP	UDP
Connection	P2P, connection orientated	Connectionless
Function	Connection based	Used for message transport and transfer
Usage	High reliability transmission	Fast, efficient transmission time
Reliability	Yes (rdt)	None
Packet Ordering	In-order	Out-of-order
Speed of Transfer	Slow	Fast (best effort)
Data Flow Control	Set window size	None
Error Checking	Yes, and recovery	Yes, no recovery
Handshake	3-Way (SYN, SYN-ACK, ACK)	None (connectionless)
Examples	HTTP, telnet, ssh, ftp, smtp	VoIP, DHCP, DNS

UDP is best suited for multimedia communications as its

- Faster
- Reliability, out of order transfer and error recovery isn't as important
- Doesn't need to be connection orientated