CS3031 – Advanced Telecommunications
2018 Exam Solutions

Question 1

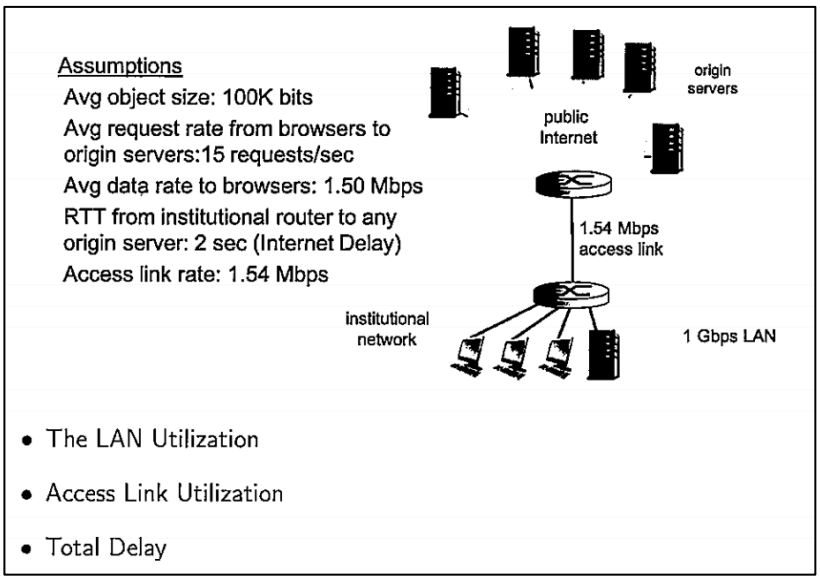
a) What is the role of a "web proxy" in a large institutional network? What are the main advantages of installing a proxy server?

The role of a web proxy in a large institutional network is to serve as an intermediary between incoming connections and the destination servers.

Proxy servers help improve web performance by storing a copy of frequently used webpages in a local cache on the proxy server. When a client requests a webpage stored in the proxy server's cache, it is provided by the proxy server which is faster than relaying the request to the desired web server to fetch the page on every occurrence. Proxy servers also help improve security by filtering out some web content and malicious software.

Proxy servers also allow for requests to be blocked dynamically as well as sites, protocols and ports.

b) Given the network and associated assumptions in the figure below calculate:



- Object Size = 100K bits
- Request Rate = 15 req/s
- Data Rate to Browsers = 1.5 Mb/s
- RTT from Institution Router to Origin Server = 2 sec
- Access Link Rate = 1.54 Mb/s
- LAN Rate = 1 Gb/s

The **LAN Utilization** can be considered as:

$$LAN\ Utilization = \frac{Data\ Rate\ to\ Browsers}{LAN\ Rate}$$

$$LAN\ Utilization = \frac{1.5\ Mb/s}{1\ Gb/s}$$

$$LAN\ Utilization = \frac{1.5 * 10^6}{1 * 10^9}$$

$$LAN\ Utilization = 0.15\%$$

The **Access Link Utilization** can be considered as:

$$Access\ Link\ Utilization = \frac{Data\ Rate\ to\ Browsers}{Access\ Link\ Rate}$$

$$Access\ Link\ Utilization = \frac{1.5\ Mb/s}{1.54\ Mb/s}$$

$$Access\ Link\ Utilization = \frac{1.5 * 10^6}{1.54\ * 10^6}$$

$$Access\ Link\ Utilization \approx 97\%$$

The **Total Delay** can be considered as:

$$Total\ Delay = Internet\ Delay + Access\ Delay + LAN\ Delay$$

$$Total\ Delay = 2\ sec + \boldsymbol{minutes} + \mu sec$$

Now assume that we install a web proxy server into the institutional network with a hit rate of 40%. Calculate:

- Access Link Utilization
- Total Delay

With the new cache, 40% of request are satisfied at cache, other 60% of requests are satisfied at origin, i.e 60% of requests will use access link. The **new Access Link Utilization** can be considered as:

$$Access\ Link\ Utilization = \frac{Data\ Rate\ to\ Browsers\ (\boldsymbol{only\ on\ cache\ miss})}{Access\ Link\ Rate}$$

$$Access\ Link\ Utilization = \frac{\boldsymbol{0.6} * 1.5\ Mb/s}{1.54\ Mb/s}$$

$$Access\ Link\ Utilization = \frac{0.9}{1.54} = \boldsymbol{58}\%$$

The **new Total Delay** can be considered as:

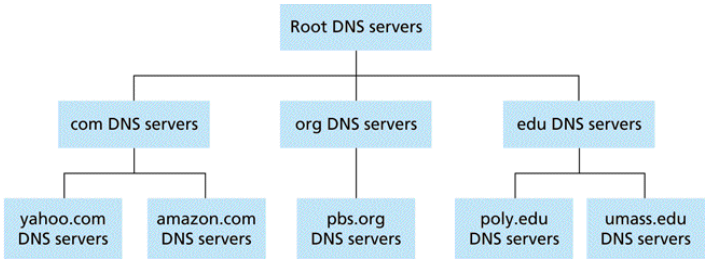
$$Total\ Delay = 0.6 * (Delay\ From\ Origin\ Servers) + 0.4 * (Delay\ From\ Cache)$$

$$Total\ Delay = 0.6 * (2\,\text{sec} + ms\ for\ Access\ Link\ and\ LAN) + 0.4 * (\mu\,\text{sec}\ for\ LAN)$$

$$Total\ Delay \approx 1.2\ sec$$

This shows that by using a web cache you can reduce the access link utilization greatly and as a result reduce the total delay all at a much cheaper cost than expanding the access link.

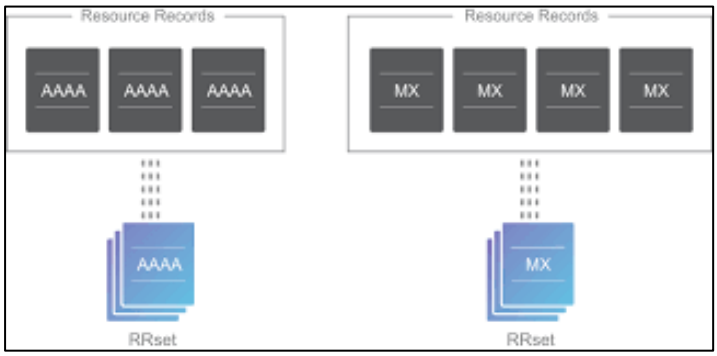
c) Describe the basic server hierarchy within the domain name system (DNS). Describe how DNSSEC validation takes place within a zone by detailing various Resource Records (RR), RRsets and Signature Keys that are required to secure a domain.



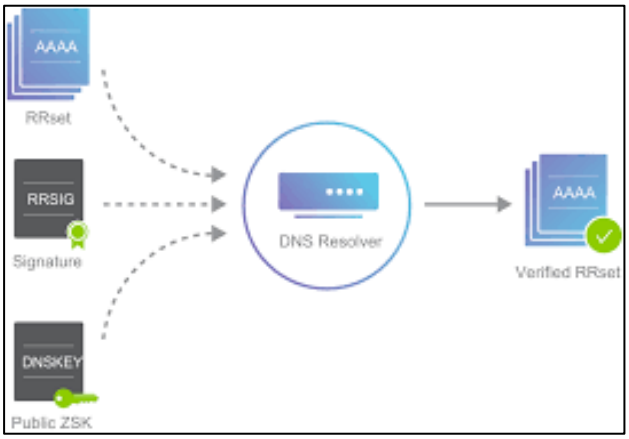
The basic server hierarchy within the domain name system (DNS) is detailed as above.

DNSSEC provides origin authentication and integrity assurance services for DNS data. This prevents malicious attackers from spoofing DNS responses and redirecting users to malicious websites (e.g fake bank login page).

The first step towards securing a zone with DNSSEC is to group all the records with the same type into a resource record set (RRset).



Each zone in DNSSEC has a zone-signing key pair (ZSK). A zone operator creates digital signatures for each RRset using the private ZSK. Zone operators must also make their public ZSK available by adding it to their name server in a DNSKEY record. When a DNSSEC resolver requests a particular record type (e.g AAAA), the name server also returns the corresponding RRSIG.



d) What is a "websocket" and what are its advantages over technologies such as AJAX and Comet? Why are websockets more efficient than traditional HTTP exchanges? Explain.

Websockets allow a long-held TCP socket connection to be established between the client and server which allows bi-directional, full duplex, messages to be instantly distributed with little overhead resulting in a very low latency connection.

Websockets don't fully replace AJAX, which should still be used for making short-lived web service calls. Unlike AJAX, WebSockets are based around an event model. The client and server can emit events and send data to each other whenever they want to. Whilst with AJAX each request must be followed by a response in a one-directional manner. Similar to AJAX, WebSockets must establish a connection with the server, however WebSockets only have to perform this once whilst with AJAX it must be done with every request causing high overhead latency.

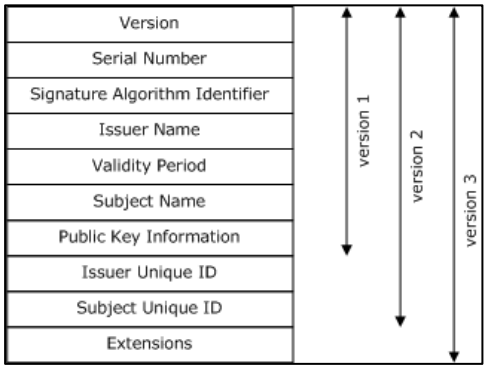
Comet is a protocol that allows '**Sever push**' behaviour wherein a server pushes events to a clients browser. It allows for the server to stream events to a client over a single persistent connection. It also allows for long polling where the browser polls the server for new events with a persistent request that is held open until it gets a response. WebSockets can be considered an extension upon Comet that allows for bi-directional pushing of events both to and from the client and server. This removes the need for long polling and significantly reduces the combined overhead of the communication.

e) Describe in detail the main components of a X.509 certificate. Explain the "handshake" procedure used in the Secure Sockets Layer (SSL) protocol to establish a secure tunnel between web browser and server.

The main components of a X.509 certificate are:

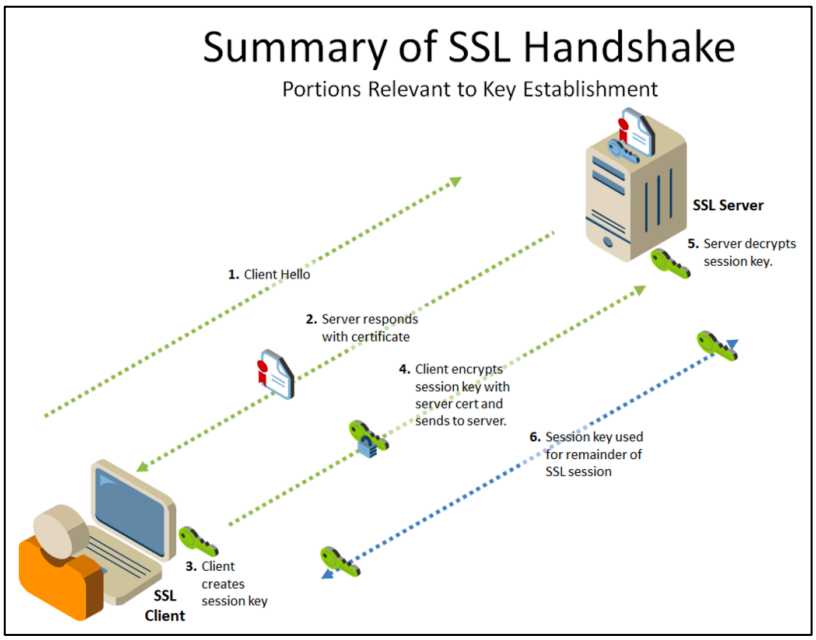
- Version: Which X.509 version applies to the certificate.
- Serial Number: Unique ID of cert assigned by CA.
- Algorithm Information: Information on signing algorithms used (e.g SHA-256).
- Issuer Name: Name of Certificate Authority (CA) issuing certificate.
- Validity Period: How long the cert is valid for.

- Subject Distinguished Name: Identity of the issued client.
- Subject Public Key Information: Clients public key information.



Within the Secure Socket Layer protocol (SSL) there are four main steps:

1. Server Authentication
2. Negotiation (agree on crypto algorithms)
3. Establish Keys
4. Client Authentication (optional)



1. A browser requests a secure page.
2. The web server sends its public key with its certificate.
3. The browser checks that the certificate was issued by a trusted root authority or Certificate Authority and that the certificate is still valid and that the certificate is related to the site contacted.
4. The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
5. The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.

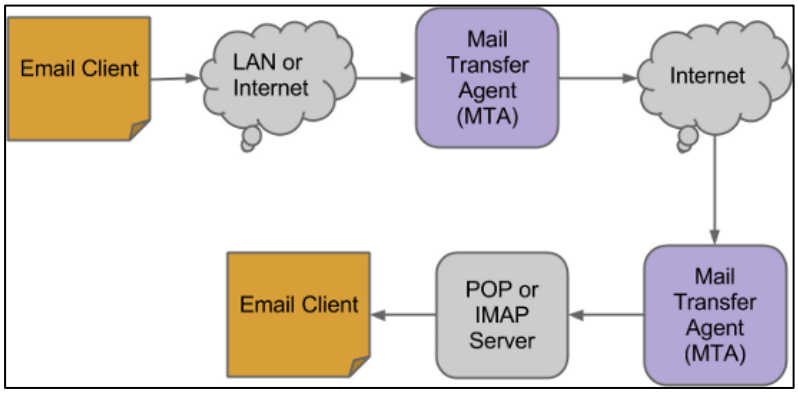
6. The browser decrypts the http data and html document using the symmetric key and displays the information.

Question 2

a) List the main components of an electronic mail system and describe the functionality of each of them. Distinguish between POP, IMAP and Webmail protocols. What do you understand by the term "stateless protocol". Is IMAP stateless?

There are four major components in an electronic mail system:

1. **Mail User Agent:** The mail user agent is an application which is used to compose, send and receive emails.
2. **Mail Transfer Agent:** The mail transfer agent is responsible for receiving incoming mail and deliver outgoing messages.
3. **Mail Host & Mailboxes:** The mail host is a server that is responsible for delivering and receiving mail for a host or a network. The mail host collects all mail sent to the domain and stores it in a specific mailbox. Once mail has been stored it can be accessed via the agent or using protocols such as POP or IMAP.
4. **Domain Name System (DNS):** The DNS plays a large role in the delivery of email. In order to deliver mail from one site to another the MTA will look up the remote site in DNS to determine which host will receive mail for the destination. In addition to mapping hostnames to IP addresses DNS stores information specific to mail delivery known as MX records.



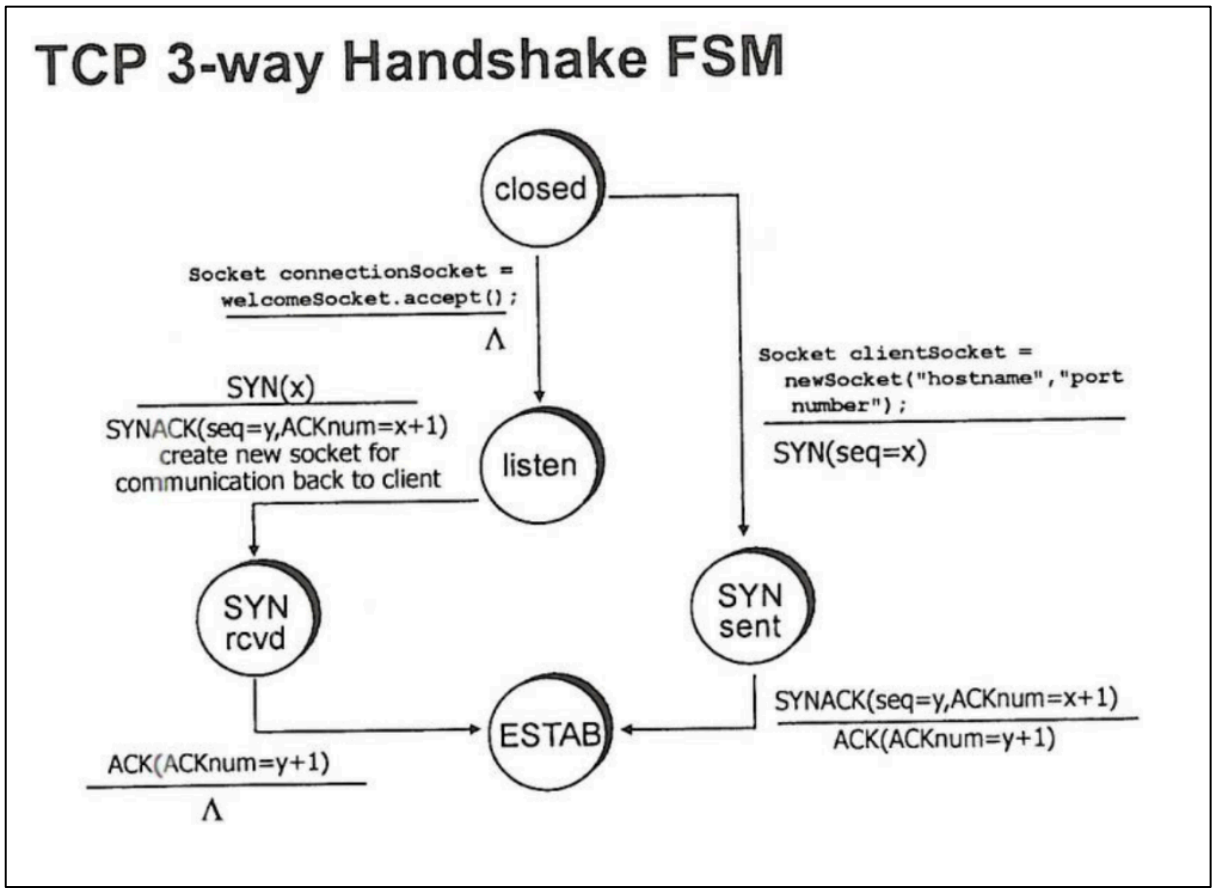
Webmail is the likes of Gmail, Outlook etc. which fully host and provide all components of an electronic mail system without the end user having to worry about any of the underlying technologies.

Post Office Protocol (POP) offers a way of interacting with mail servers that dates back to an archaic internet. Back then computers did not have permanent access, they connected to the internet, did what they needed to do and disconnected. The connections were also pretty low bandwidth. POP works as you'd expect it connects to the mail server, downloads all messages that have not been previously downloaded, and then it pops off and disconnects.

Internet Messaging Access Protocol (IMAP) is a protocol that is more suited to the modern day internet. The idea behind IMAP is that it keeps users from having to be tied to a single email client and gives them the ability to read their emails as if they were in the cloud. IMAP, unlike POP3, stores all messages on the server, allowing a client to read all emails until they are deleted. Metadata is also stored on the server such as which emails have been read.

Stateless Protocols are protocols that have no stored memory or state. They are brought up with an initial state that is independent of any previous actions (it does not remember history). IMAP **is not** a stateless protocol as it stores information regarding what emails have been read and by who.

b) Draw the finite state machine (FSM) for the 3-way TCP handshake from both the client and server perspectives. You are required to detail the state transitions in the FSM.



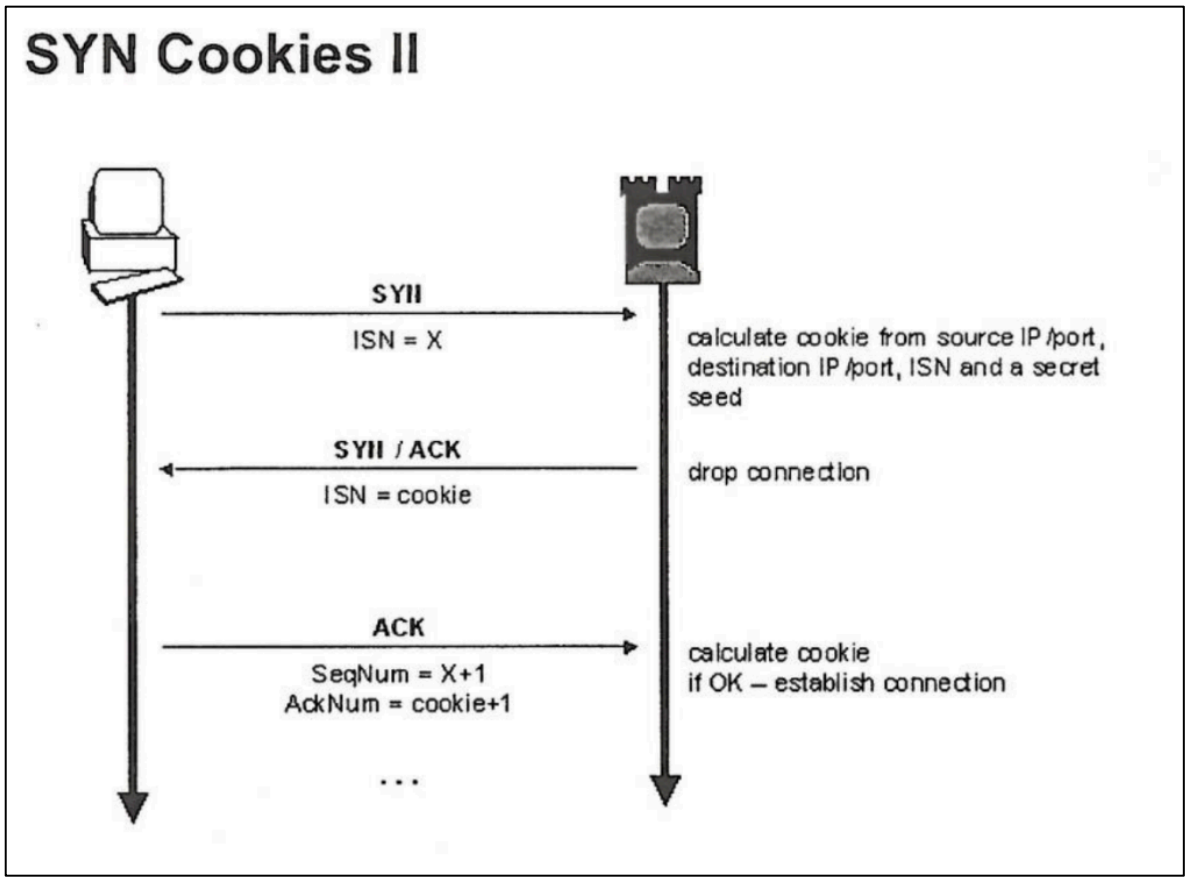
c) What is the "SYN Flood Attack" in TCP. Describe in detail as to how this attack can be mitigated using "SYN Cookies".

SYN Flood Attacks is when an attacker sends a large number of TCP SYN segments (looking to establish a connection) without completing the third handshake step. This causes the server to allocate space in memory for the incomplete connection and cause a memory overflow and ultimately crash.

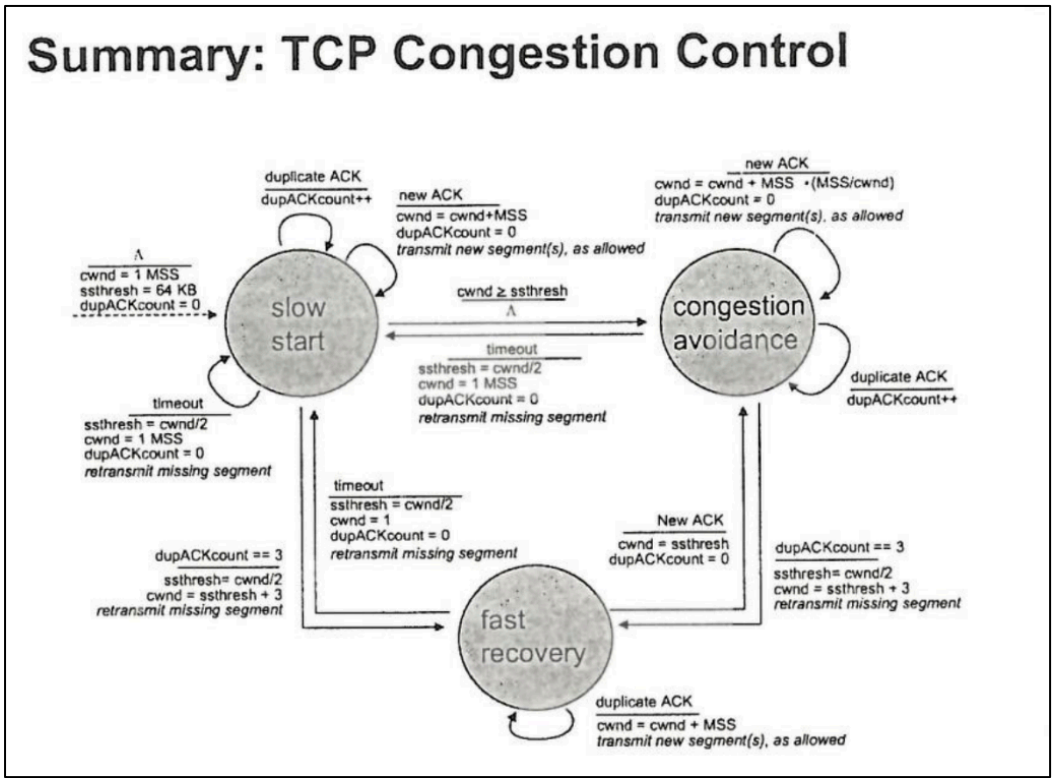
SYN Cookies allow for the server to determine if SYN segments are coming from a legitimate user. Server creates an initial sequence number (**ISN/Cookie**) from the hash of:

- Source IP address & port
- Dest IP address & port
- Secret seed

The server then sends a **SYNACK** whilst dropping the connection and maintaining no state info about the corresponding SYN. A legitimate client will then return an ACK segment using the cookie information (**ISN+1**) in the ACK.

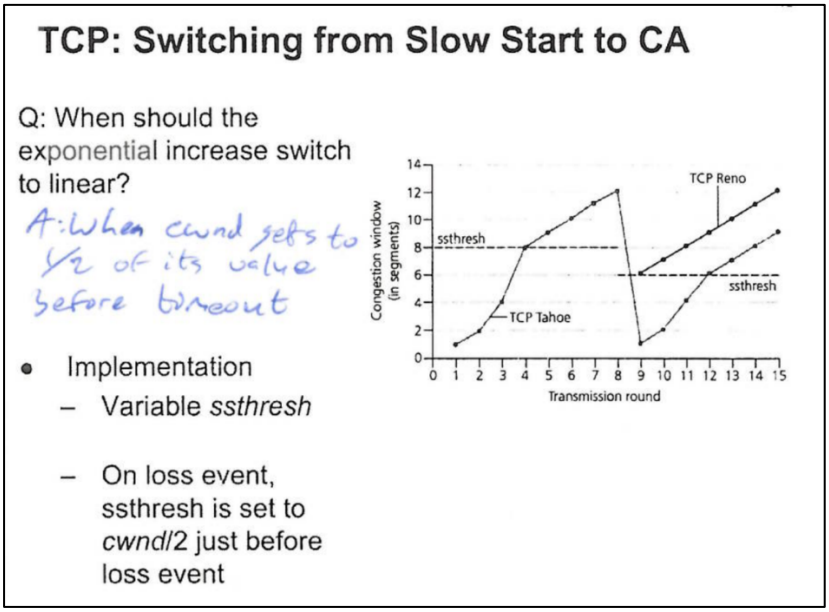


d) With the help of an FSM describe the main building blocks of the TCP Congestion Control Algorithm.



- When connection begins, increase rate exponentially until first loss event.
- Double **cwnd** every RTT (for every ACK received at sender).
- Window grows exponentially to **sstresh** then grows linearly.
- Loss indicated by 3 duplicate ACKs.

- **TCP Reno:** Cut **cwnd** in half and grow linearly from here (set **sstresh** to half also).
- **TCP Tahoe:** If timeout, set **sstresh** to half and **cwnd** back to one.



e) What is Fermat's Little Theorem and why is it useful in the context of primality testing? Show that 29 is a prime number using Fermat's theorem. In the context of primality testing Fermat's Little Theorem can produce false positives. What can be done to mitigate this problem?

Fermat's Little Theorem allows us to determine if a given randomly generated number is prime. A simple primality test can be based on Fermat's Little Theorem:

- $a^p \equiv a \ (mod \ p)$
- $a^{p-1} \equiv 1 \ (mod \ p)$

However, there are certain composite numbers which may fulfil the above condition (aka the Charmichael numbers). In order to detect them, the algorithm runs *s* times with different values of $a \ \in \{2, \dots, p-2\}$

Exercise – Show that 29 is a prime number using Fermat's theorem:

Using the values a = 2 and p = 29:

$$2^{28} \equiv 1 \ (mod \ 29)$$

$$\mathbf{268,435,456 \equiv 1 \ (mod \ 29)}$$

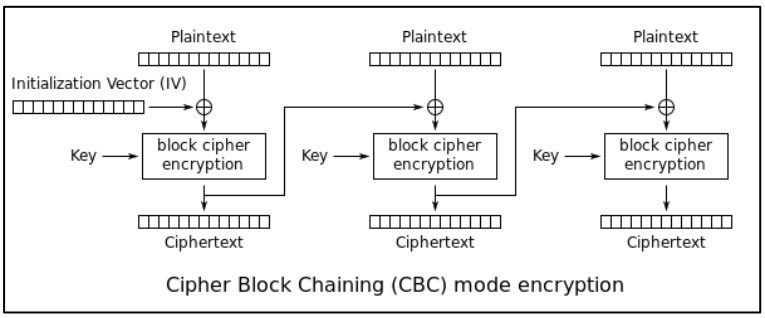
This is true and therefore we can infer 29 is a prime number. For further confidence you would test this with more values of a.

Question 3

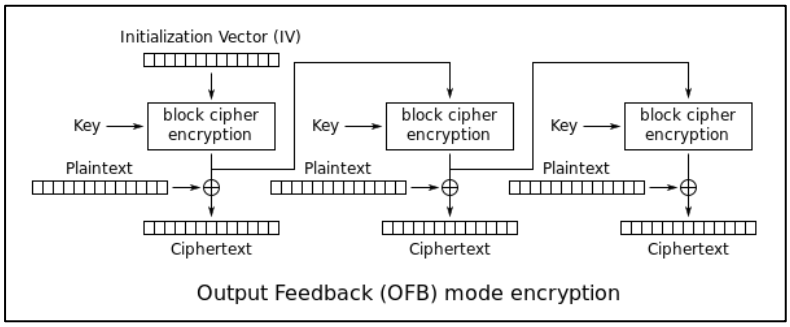
a) Describe the electronic code book (ECB) mode used in the DES cipher. Explain how the cipher block chaining (CBC) mode overcomes the block substitution attack of ECB mode. Explain why the output feedback mode (OFB) is described as being a "synchronous stream cipher".

Electronic Code Book (ECB) mode used in the DES cipher is when the plaintext is operated upon independently in 64 bit (8 byte) chunks at a time. Using a 56-bit key and the DES encryption algorithm each 64 bit chunk is encrypted. This can be performed in parallel. However, this is a bad thing as ECB mode encrypts in a highly deterministic manner. Identical plain text blocks result in identical ciphertext blocks. This can allow for a substitution attack to occur as each block is independent of any other block. Therefore, no one will notice if an attacker changes any of the blocks (i.e bank address).

Cipher Block Chaining (CBC) mode is when each block of plaintext is XOR'd with the previous ciphertext block after it has been encrypted. The initial block is XOR'd with an Initialisation Vector (IV). This mode introduces a dependency as each ciphertext block depends on all plaintext blocks processed up to that point. If one block is changed, the resulting following ciphertext blocks will be corrupted.



Output Feedback Mode (OFB) is described as being a *"synchronous stream cipher"* as within OFB a block cipher encryption is used to create a stream cipher encryption scheme. The output of the cipher outputs b key stream bits, where b is the width of the block cipher used. Each plaintext digit is then encrypted one at a time with the corresponding digit in the keystream.



b) Computing modular exponentiation efficiently is inevitable for practicability of RSA. Compute the following exponentiation x^e mod m by applying the square and multiply algorithm:

x=2, 3=79, m = 101

The aim of the game here is to compute:

$$2^{79}\ mod\ 101$$

First compute 2^1:

$$2^1 = 2 \rightarrow \mathbf{2\ mod\ 101}$$

Now square both sides of the exponentiation:

$$2^2 = (2^1)^2$$

$$2^2 = 4 \rightarrow \mathbf{4\ mod\ 101}$$

Square both sides again:

$$2^4 = (2^2)^2$$

$$2^4 = 16 \rightarrow \mathbf{16\ mod\ 101}$$

Square both sides again:

$$2^8 = (2^4)^2$$

$$2^8 = 256 \rightarrow \mathbf{54\ mod\ 101}$$

Square both sides again:

$$2^{16} = (2^8)^2$$

$$2^{16} = (54)^2\ mod\ 101$$

$$2^{16} = 2916\ mod\ 101$$

$$2^{16} = \mathbf{88\ mod\ 101}$$

Square both sides again:

$$2^{32} = (2^{16})^2$$

$$2^{32} = (88)^2\ mod\ 101$$

$$2^{32} = 7744\ mod\ 101$$

$$2^{32} = \mathbf{68\ mod\ 101}$$

Square both sides again:

$$2^{64} = (2^{32})^2$$

$$2^{64} = (68)^2\ mod\ 101$$

$$2^{64} = 4624\ mod\ 101$$

$$2^{64} = \mathbf{79\ mod\ 101}$$

If we were to square both sides again we would exceed 2^{79} therefore we terminate our execution here. We then write down our results:

2^1	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}
2 mod 101	**4** mod 101	**16** mod 101	**54** mod 101	**88** mod 101	**68** mod 101	**79** mod 101

Now, write our original exponent (79) in binary:

$$79_2 = 1001111$$

$$79 = 64 + 8 + 4 + 2 + 1$$

Then, using our above table we can represent this as:

$$2^{79} = 2^{64+8+4+2+1}$$

$$= (2^{64})(2^8)(2^4)(2^2)(2^1)$$

$$= (79)(54)(16)(4)(2)\ mod\ 101$$

$$= 546048\ mod\ 101$$

$$= 42\ mod\ 101$$

c) What are the distinguishing characteristics of a Group? What is the order ord(a) of a group (G, o)? Determine the order of a=3 in $\mathbb{Z}^*_{11}$. Let G be a finite cyclic group. Find the number of primitive elements in $\mathbb{Z}^*_5$.

A group is a set of elements with one operation and the corresponding inverse operation. If the operation is addition, the inverse is subtraction. If the operation is multiplication, the inverse is division.

The order **ord(a)** of an element of group (G, o) is the smallest positive integer k such that:

- $a^k = a * a * \ldots * a = e$ where e is the **identity element**

For example the ord(a) of an element of the group (G, mod n) is:

- $a^k = a * a * \ldots * a = 1\ mod\ n$

To determine the order of a=3 in $\mathbb{Z}^*_{11}$ we keep computing the powers of a until we find the identity element (1 mod 11).

- $a^k = a * a * \ldots * a = 1\ mod\ n$
- $3^1 = 3 \equiv 3\ mod\ 11$
- $3^2 = 9 \equiv 9\ mod\ 11$
- $3^3 = 27 \equiv 5\ mod\ 11$
- $3^4 = 81 \equiv 4\ mod\ 11$
- $\mathbf{3^5 = 243 \equiv 1\ mod\ 11}$

We have now found the power of a (3) that results in our identity element. We can now also say:

$$\boldsymbol{ord(3) = 5}$$

The number of primitive elements in a finite cyclic group can be found using the following rules:

- The number of primitive roots of G is $\phi(|G|)$
- If |G| is prime, then all elements $a \neq 1 \in G$ are primitive

To find the number of elements in $\mathbb{Z}^*_5$ we must first calculate |G|. Since 5 is a prime number we can infer the following:

$$|\boldsymbol{G}| = \mathbf{5} - \mathbf{1} = \mathbf{4}$$

We must then use Euler's totient function ϕ to calculate the number of primitive roots:

$$\phi(m) = \prod_{i=1}^{n} (p_i{}^{e_i} - p_i{}^{e_i - 1})$$

$$\phi(|G|) = \phi(4) = 4 * \left(1 - \frac{1}{2}\right) = 2$$

Therefore, the number of primitive elements in $\mathbb{Z}^*_5$ is 2, namely:

$$\{1, 3\}$$

d) Given the elliptic curve E over $\mathbb{Z}^*_{17}$ with base point P=(5,1):

$$E: y^2 = x^3 + 4x + 20 \ mod \ 17$$

Calculate the following point multiplication 2P using the formulas provided below:

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

$$2P = P + P = (5,1) + (5,1) = (x_3, y_3)$$

$$\boldsymbol{s = \frac{3(x_1)^2 + a}{2(y_1)}}$$

$$s = \frac{3(5)^2 + 4}{2(1)} mod \ 17 = \frac{79}{2} \ mod \ 17$$

$$\boldsymbol{s = 5.5}$$

$$\boldsymbol{x_3 = s^2 - x_1 - x_2 \; mod \; p}$$

$$x_3 = (5.5)^2 - 5 - 5 \; mod \; 17$$

$$x_3 = 20.25 \; mod \; 17$$

$$\boldsymbol{x_3 = 3.25}$$

$$\boldsymbol{y_3 = s(x_1 - x_3) - y_1 \; mod \; p}$$

$$y_3 = 5.5(5 - 3.25) - 1 \; mod \; 17$$

$$y_3 = 8.625 \; mod \; 17$$

$$\boldsymbol{y_3 = 8.625}$$

$$\boldsymbol{\therefore 2P = (3.25, 8.625)}$$