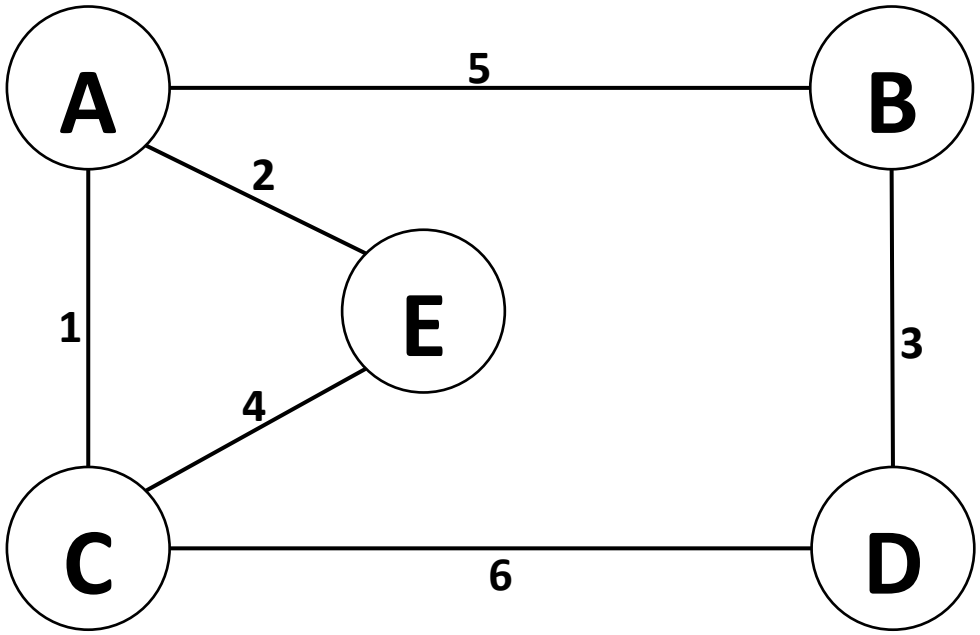
Q1) A network is described by the following routers and link weights:
(A, B, 5), (A, C, 1), (A, E, 2), (B, D, 3), (C, D, 6), (C, E, 4)

1) Show, step-by-step (i.e. after each round of broadcasting), how the routing tables for each router would be generated using distance vector routing (assume all routers are freshly rebooted and a round consists of router A first broadcasting its routing table (and all neighbours updating their routing tables), then router B, continuing in alphabetical order until all routers have broadcast) i.e., a round of broadcasting means that each router has broadcast its routing table once.

Answer:
The network diagram is given below:



Routing Table For A		
Destination	Next Hop	Cost
A	-	0
B	B	5
C	C	1
D		
E	E	2

Routing Table For B		
Destination	Next Hop	Cost
A	A	5
B	-	0
C		
D	D	3
E		

Routing Table For C		
Destination	Next Hop	Cost
A	A	1
B		
C	-	0
D	D	6
E	E	4

Routing Table For D		
Destination	Next Hop	Cost
A		
B	B	3
C	C	6
D	-	0
E		

Routing Table For E		
Destination	Next Hop	Cost
A	A	2
B		
C	C	4
D		
E	-	0

Round 1:

Router A broadcasts its table to B, C and E.

Routing Table For B			
Destination	Next Hop	Cost	Update
A	A	5	
B	-	0	
C	A	6	Updated by A
D	D	3	
E	A	7	Updated by A

Routing Table For C			
Destination	Next Hop	Cost	Update
A	A	1	
B	A	6	Updated by A
C	-	0	
D	D	6	
E	A	3	Updated by A

Routing Table For E			
Destination	Next Hop	Cost	Update
A	A	2	
B	A	7	Updated by A
C	A	3	Updated by A
D			
E	-	0	

Round 2:

Router B broadcasts its table to A and D.

Routing Table For A			
Destination	Next Hop	Cost	Update
A	-	0	
B	B	5	
C	C	1	
D	B	8	Updated by B
E	E	2	

Routing Table For D			
Destination	Next Hop	Cost	Update
A	B	8	Updated by B
B	B	3	
C	C	6	
D	-	0	
E	B	10	Updated by B

Round 3:

Router C broadcasts its table to A, D and E.

Routing Table For A			
Destination	Next Hop	Cost	Update
A	-	0	
B	B	5	
C	C	1	
D	C	7	Updated by C
E	E	2	

Routing Table For D			
Destination	Next Hop	Cost	Update
A	C	7	Updated by C
B	B	3	
C	C	6	
D	-	0	
E	C	9	Updated by C

Routing Table For E			
Destination	Next Hop	Cost	Update
A	A	2	
B	A	7	Updated by A
C	A	3	Updated by A
D	A	9	Updated by C
E	-	0	

Round 4:

Router D broadcasts its table to B and C.

Routing Table For B			
Destination	Next Hop	Cost	Update
A	A	5	
B	-	0	
C	A	6	Updated by A
D	D	3	
E	A	7	Updated by A

Routing Table For C			
Destination	Next Hop	Cost	Update
A	A	1	
B	A	6	Updated by A
C	-	0	
D	D	6	
E	A	3	Updated by A

Round 5:

Router E broadcasts its table to A and C.

Routing Table For A			
Destination	Next Hop	Cost	Update
A	-	0	
B	B	5	
C	C	1	
D	C	7	Updated by C
E	E	2	

Routing Table For C			
Destination	Next Hop	Cost	Update
A	A	1	
B	A	6	Updated by A
C	-	0	
D	D	6	
E	A	3	Updated by A

So, the final routing table of each router would be:

Routing Table For A		
Destination	Next Hop	Cost
A	-	0
B	B	5
C	C	1
D	C	7
E	E	2

Routing Table For B		
Destination	Next Hop	Cost
A	A	5
B	-	0
C	A	6
D	D	3
E	A	7

Routing Table For C		
Destination	Next Hop	Cost
A	A	1
B	A	6
C	-	0
D	D	6
E	A	3

Routing Table For D		
Destination	Next Hop	Cost
A	C	7
B	B	3
C	C	6
D	-	0
E	C	9

Routing Table For E		
Destination	Next Hop	Cost
A	A	2
B	A	7
C	A	3
D	A	9
E	-	0

2) How many rounds of broadcasting the routing tables are required before each router's table is optimal?

Answer:
Here, we can see that, there is not any update created by router table D and E from round 4 and round 5. So, we can see that, we are required at least 3 rounds of broadcasting the routing tables before each router's table is optimal.

Q2) You have been asked to set up a TCP/IP-based network that must support at least 3628 nodes.

1) Define an appropriate subnet mask to support such a network. The mask must provide for the maximum number of network identifiers while still supporting the required number of nodes. Express your answer in dotted decimal notation.

Answer:

To support at least 3628 nodes, we need to determine the minimum number of bits required for the host part of the IP address. The formula to calculate this is:

Number of Hosts = $2^n - 2$

Where,

n is the number of bits for the host part, and we subtract 2 because the first and last addresses in a subnet are reserved for network address and broadcast address.

For 3628 nodes: 211 < 3628 < 212

So, we will need at least 12 bits for the host part.

Since IPv4 addresses are 32 bits in total and we're using 12 bits for the host part, that leaves 20 bits for the network part.

Converting 20 bits to dotted decimal notation for the subnet mask:

Subnet Mask = 11111111.11111111.11110000.00000000

This translates to: 255.255.240.0

So, the appropriate subnet mask to support at least 3628 nodes is 255.255.240.0.

2) Given that the network ID is 10.158.192.0, provide the physical network identity in CIDR notation.

Answer:

To determine the required CIDR notation for the physical network identity, we need to calculate the number of bits needed to accommodate at least 3628 nodes. The formula to calculate the number of host bits needed is:

Number of Host Bits = $\log_2$(Number of Nodes + 2) Here, 2 is added because the first and last addresses in a subnet are reserved for network address and broadcast address.

So, for 3628 nodes:

Number of Host Bits = $\log_2(3628+2) = \log_2(3630) \approx 11.83$

Since we can't have a fraction of a bit, we round up to the next whole number. So, we need at least 12 bits to accommodate 3628 nodes.

Now, we subtract these host bits from the total 32 bits in IPv4 to find the number of network bits:

Number of Network Bits = 32 − Number of Host Bits = 32 – 12 = 20

So, the CIDR notation for the physical network identity is 10.158.192.0/20.

3) Calculate the full IP address of node 1537 in this network.

Answer:
Given network id is 10.158.192.0.
To calculate the full IP address of node 1537 in this network we add the decimal representation of node 1537 to the network id. However, since IP addresses are represented in binary, we'll first find the binary representation of both node and network id.
So, network id 10.158.192.0 = 00001010.10011110.11000000.00000000
And node 1537 = 11000000001
Since it is 11 bits, we need to add leading zeros to make it 12 bits to match our host bits and then doing suitable padding.
So, it becomes 00000110.00000001.
Now, adding both,
00001010.10011110.11000000.00000000 + 00000110.00000001
= 00001010.10011110.11000110.00000001
which in decimal would be 10.158.198.1.
So, the full IP address of node 1537 in this network is 10.158.198.1.

Q3) TCP and UDP are two of the most frequently used Transport Layer protocols.

1) What are the main differences between TCP and UDP?

Answer:

The main differences between TCP and UDP are listed below:

- **Connection-Oriented vs. Connectionless:** TCP (Transmission Control Protocol) is connection-oriented which establishes a connection before transmitting data and ensures reliable delivery through acknowledgments and retransmissions whereas, UDP (User Datagram Protocol) is connectionless which does not establish a connection before sending data and does not guarantee delivery.
- **Reliability:** TCP ensures reliable delivery by retransmitting lost packets and ensuring they arrive in order whereas, UDP does not guarantee delivery or order of packets.
- **Packet Header Size:** TCP header is larger due to its features like sequencing, acknowledgment, and flow control whereas, UDP header is smaller.
- **Flow Control and Congestion Control:** TCP implements flow control and congestion control mechanisms to manage data flow and prevent network congestion whereas, UDP does not have these mechanisms.
- **Usage:** TCP is commonly used for applications requiring reliable and ordered delivery of data, such as web browsing, email, file transfer (FTP), etc whereas, UDP is used for applications where speed and efficiency are more critical than reliability, such as online gaming, video streaming, DNS (Domain Name System) queries, etc.

2) When would using TCP be preferable to using UDP? Give two examples.

Answer:

TCP is preferred over UDP when reliability, ordered delivery, and error recovery are critical for the application or service being provided. For example,

- **File Transfer:** When transferring large files over the internet, such as software updates or multimedia files, using TCP ensures that all parts of the file are reliably delivered and in the correct order.
- **Web Browsing:** TCP is preferred for web browsing because it ensures that web pages are displayed correctly by reliably delivering HTML, CSS, and other resources.

3) When would using UDP be preferable to using TCP? Give two examples.

Answer:

UDP is preferred over TCP when speed, low latency, and reduced overhead are more important than reliability and ordered delivery. For example,

- **Real-Time Communication:** Applications that require real-time communication, like online gaming or VoIP (Voice over Internet Protocol), often use UDP because it offers lower latency and overhead compared to TCP.
- **Multimedia Streaming:** UDP is commonly used for multimedia streaming, such as video streaming or live broadcasting, where a few dropped packets are acceptable, but low latency is crucial for maintaining smooth playback.

Q4) For the following cyphertext:

```
Fgxywfhy kwtrymjB npnujinf jsywdts" JsnlrfRf
hmnsj":Y mjJsnlrf rfhmnsjn xfhnumjw ijanhjij
ajqtujif sizxjins ymjjfwqd -ytrni-2 0ymhjsyz
wdytuwty jhyhtrrj whnfq,in uqtrfynh ,fsirnqn
yfwdhtrr zsnhfynt s.Nybfxj ruqtdjij cyjsxnaj
qdgdSfen Ljwrfsdi zwnslBtw qiBfwNN, nsfqqgwf
shmjxtky mjLjwrfs rnqnyfwd .YmjJsnl rfrfhmns
jbfxhtsx nijwjixt xjhzwjym fynybfxz xjiytjsh
numjwymj rtxyytu- xjhwjyrj xxfljx.Y mjJsnlrf
mfxfsjqj hywtrjhm fsnhfqwt ytwrjhmf snxrymfy
xhwfrgqj xymj26qj yyjwxtky mjfqumfg jy.Nsydu
nhfqzxj, tsjujwxt sjsyjwxy jcytsymj Jsnlrf'x
pjdgtfwi fsifstym jwujwxts bwnyjxit bsbmnhmt
kymj26qn lmyxfgta jymjpjdg tfwinqqz rnsfyjif
yjfhmpjd uwjxx.Nk uqfnsyjc ynxjsyjw ji,ymjnq
qzrnsfyj iqjyyjwx fwjymjhn umjwyjcy .Jsyjwns
lhnumjwy jcyywfsx ktwrxnyg fhpnsytw jfifgqju
qfnsyjcy .Ymjwtyt wrjhmfsn xrhmfslj xymjjqjh
ywnhfqht ssjhynts xgjybjjs ymjpjdxf siymjqnl
myxbnymj fhmpjduw jxx.Ymjx jhzwnydt kymjxdxy
jrijujsi xtsrfhmn sjxjyyns lxymfybj wjljsjwf
qqdhmfsl jiifnqd, gfxjitsx jhwjypjd qnxyxinx
ywngzyji nsfiafsh j,fsitst ymjwxjyy nslxymfy
bjwjhmfs ljiktwjf hmrjxxfl j.Ymjwjh jnanslxy
fyntsbtz qimfajyt pstbfsiz xjymjjcf hyxjyyns
lxjruqtd jigdymjy wfsxrnyy nslxyfyn tsytxzhh
jxxkzqqd ijhwduyf rjxxflj. BmnqjSfe nLjwrfsd
nsywtizh jifxjwnj xtknruwt ajrjsyxy tymjJsnl
rftajwym jdjfwx,f siymjxjm frujwjii jhwduynt
sjkktwyx ,ymjdini styuwjaj syUtqfsi kwtrhwfh
pnslymjr fhmnsjfx jfwqdfxI jhjrgjw1 932fsiwj
finslrjx xfljxuwn twytfsin sytymjbf w.Utqfsi
'xxmfwns ltkymjnw fhmnjajr jsyxjsfg qjiymjFq
qnjxytjc uqtnyJsn lrf-jshn umjwjirj xxfljxfx
frfotwxt zwhjtkns yjqqnljs hj.Rfsdh trrjsyfy
twxxfdym jkqtbtkZ qywfhtrr zsnhfynt sxnsyjqq
nljshjkw trymjijh wduynslt kJsnlrf, Qtwjse,f
sitymjwh numjwxxm twyjsjiy mjbfwxzg xyfsynfq
qdfsirfd jajsmfaj fqyjwjin yxtzyhtr j.
```

1) Describe your analysis to determine the classical cipher used and break the cipher.

Answer:

Here, for the analysis of given encrypted code, my first task was to determine whether it is a Transposition (Column) or Substitution (Caesar or Vigenere) cipher. So, to determine it, I compared the frequency of letters in the ciphertext with that of the plaintext English alphabet. And then, I found that in the ciphertext, the occurrence of alphabet “e” is only 3 times, and the occurrence of alphabet “o” is just 1 time. This made me believe that it should be Caesar Cipher using the key length 1. And now, while counting the frequency of all the alphabets, I found that the alphabet “j” has the highest occurrence i.e. 223 times and “y” with second highest occurrence of 148 and then “f” with third highest occurrence of 125. Now, as per the letter’s frequency used in English alphabet, I determined that the ciphertext “j” should be “e” and “y” should be “t” and “f” should be “a” and going so on for some more alphabets, I again found that there is sequencing in the alphabets and the shift of key “6” or “F” is used. Then I was somehow able to decode the above given ciphertext using JKrypto. After the decoding from JKrypto, I found that the use of

whitespaces is random, and I slowly started to fix it out by myself. Finally, after this, I was successful in getting the result which seems to be accurate.

2) Provide the corresponding plaintext.

Answer:

Abstract from the Wikipedia entry on "Enigma Machine": The Enigma machine is a cipher device developed and used in the early-to-mid-20th century to protect commercial, diplomatic, and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages. The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plaintext is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each key press. The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt a message. While Nazi Germany introduced a series of improvements to the Enigma over the years, and these hampered decryption efforts, they did not prevent Poland from cracking the machine as early as December 1932 and reading messages prior to and into the war. Poland's sharing of their achievements enabled the Allies to exploit Enigma-enciphered messages as a major source of intelligence. Many commentators say the flow of Ultra communications intelligence from the decrypting of Enigma, Lorenz, and other ciphers shortened the war substantially and may even have altered its outcome.

Q5) Many data breaches occur because people use bad passwords. Others occur because passwords are stored incorrectly.

1) Describe some current best practices for ensuring users select reasonable passwords (include a reference to at least one source).

Answer:

According to National Institute of Standards and Technology (NIST) Special Publication 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management", *(link provided)* the current best practices for ensuring users select reasonable passwords involve educating users on password complexity and implementing password policies that encourage strong passwords. Here are some key practices:

- **Use Passphrases:** Encourage users to create passphrases instead of passwords. Passphrases are longer and easier to remember, yet more secure than traditional passwords.
- **Password Complexity:** Require passwords to include a mix of upper-case and lower-case letters, numbers, and special characters. This increases the complexity and difficulty of guessing or cracking passwords.
- **Password Length:** Encourage users to create longer passwords. Longer passwords are generally more secure as they provide more possible combinations for attackers to guess.
- **Avoid Common Passwords:** Discourage the use of common passwords and easily guessable information such as "password123" or "qwerty".
- **Password Managers:** Encourage the use of password managers to generate and store complex passwords securely. Password managers can help users maintain unique passwords for each service without the need to remember them all.

2) Describe some current best practices for authenticating through the use of passwords (e.g., how a service provider can verify a password entered by a user) (include a reference to at least one source).

Answer:

According to OWASP (Open Web Application Security Project) Cheat Sheet Series for Password Storage, *(link provided)* the current best practices for authenticating through the use of passwords involve implementing secure password storage mechanisms and strong authentication protocols. Here are some key practices:

- **Salted Hashing:** Store passwords securely using a salted hash function. Salted hashing involves adding a random value (salt) to each password before hashing it. This prevents attackers from using precomputed hash tables (rainbow tables) to crack passwords.
- **Key Derivation Functions:** Use key derivation functions (KDFs) such as bcrypt, scrypt, or Argon2 for password hashing. These functions are specifically designed for password hashing and include features such as adjustable computational cost and memory hardness to make brute-force attacks more difficult.
- **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security beyond passwords. MFA typically involves combining something the user knows (password) with something they have (e.g., a mobile device or security token) or something they are (e.g., biometric authentication).
- **Rate Limiting and Account Lockout:** Implement rate limiting and account lockout mechanisms to protect against brute-force attacks. Limit the number of logins attempts within a certain time and lock user accounts temporarily after multiple failed attempts.
- **Secure Transport:** Ensure that passwords are transmitted securely over the network using HTTPS to protect against eavesdropping and man-in-the-middle attacks.