RAMAIAH UNIVERSITY OF APPLIED SCIENCES

ASSIGNMENT - 2

Course Code	CSC303A
Course Name	Computer Networks
Programme	B Tech
Department	CSE
Faculty	FET

Name of the Student	K Srikanth
Reg. No	17ETCS002124
Semester/Year	5th / 3rd Year
Course Leader/s	Dr. Rinki Sharma

Declaration Sheet				
Student Name	K Srikanth			
Reg. No	17ETCS002124			
Programme	B.Tech		Semester/Year	5th / 3rd Year
Course Code	CSC303A			
Course Title	Computer Networks			
Course Date	14/09/2020	to	16/02/2021	
Course Leader	Dr. Rinki Sharma			

Declaration

The assignment submitted herewith is a result of my own investigations and that I have conformed to the guidelines against plagiarism as laid out in the Student Handbook. All sections of the text and results, which have been obtained from other sources, are fully referenced. I understand that cheating and plagiarism constitute a breach of University regulations and will be dealt with accordingly.

Signature of the Student		Date	
Submission date stamp (by Examination & Assessment Section)			

Signature of the Course Leader and date	Signature of the Reviewer and date

Faculty of Engineering & Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	**Programme**	B. Tech.
Semester	5th		
Course Code	CSC303A	**Course Title**	Computer Networks
Course Leader	Dr. Rinki Sharma, Ms. Suvidha K S, Mr. Nithin Rao R		

Assignment - 2					
Register No.	17ETCS002124	Name of Student	K Srikanth		
Sections		**Marking Scheme**	**Max Marks**	**First Examiner Marks**	**Second Examiner Marks**
Q1	1.1	Introduction to VLSM	01		
	1.2	Difference between VLSM and CIDR	02		
	1.3	Advantages of using VLSM and CIDR together in a single network	02		
		Max Marks	**05**		
Q2	2.1	Differentiate among IEEE 802.11 Wi-Fi protocols 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax w.r.t data rate, bandwidth, frequency band and access techniques	10		
	2.2	Explain the different encryption techniques used in IEEE 802.11 Wi-Fi protocols.	10		
		Max Marks	**20**		
		Total Assignment Marks	**25**		

RAMAIAH UNIVERSITY OF APPLIED SCIENCES

Course Marks Tabulation				
Component- 1(B) Assignment	**First Examiner**	**Remarks**	**Second Examiner**	**Remarks**
Q 1				
Q 2				
Marks (Max 25)				
Signature of First Examiner			Signature of Second Examiner	

Please note:

1. Documental evidence for all the components/parts of the assessment such as the reports, photographs, laboratory exam / tool tests are required to be attached to the assignment report in a proper order.
2. The First Examiner is required to mark the comments in RED ink and the Second Examiner's comments should be in GREEN ink.
3. If the variation between the marks awarded by the first examiner and the second examiner lies within +/- 3 marks, then the marks allotted by the first examiner is considered to be final. If the variation is more than +/- 3 marks then both the examiners should resolve the issue in consultation with the Chairman BoE.

Assignment- 2

Instructions to students:

1. The assignment consists of **3** questions.
2. Maximum marks are **25.**
3. The assignment has to be neatly word processed as per the prescribed format.
4. The maximum number of pages should be restricted to **9**.
5. The printed assignment must be submitted to the course leader.
6. **Submission Date: January 22nd 2021**
7. **Submission after the due date is not permitted.**
8. **IMPORTANT**: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
9. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

Preamble

This course is intended to provide a thorough knowledge of the concepts of computer networks to students. It introduces the layered software hierarchy and the protocols that are applied at each layer. This course also touches on certain application areas of computer networks such as Local Area Networks and Mobile Ad-hoc Networks.

Question 1

Q1.1)

Introduction

In real life scenario, some subnets may require large number of host addresses while other **may require only few addresses.** Subnetting had long been a way to better utilize address space. When we perform Subnetting, all subnets have the same number of hosts, this is known as **FLSM (Fixed length subnet mask).** In FLSM all subnets use same subnet mask, this led to inefficiencies. Several new methods of addressing were created so that usage of **IP space was more efficient.** The first of these methods is called **Variable-Length Subnet Masking (VLSM).**

Variable Length Subnet Mask (VLSM) extends classic Subnetting. VLSM is a process of dividing an IP network into the **subnets of different sizes without wasting IP addresses**. It breaks down subnets into the smaller subnets, according to the need of individual networks.

Q1.2)

The IPv4 address space is generally divided into **5 classes based upon the usage and number of hosts** in the network. Each class has a specific range of IP addresses (and ultimately dictates the number of devices you can have on your network). **Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.**

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Figure 1 iPv4 Classes

Before discussing about VLSM and CIDR, let us discuss what subnetting is.

Subnets divide a single network into smaller pieces. This is done by taking bits from the host portion of the address to use in the creation of a "**sub" network**. For example, take the class B network **147.208.0.0.** The default **network mask is 255.255.0.0**, and the last two octets contain the host portion of the address. To use this address space more efficiently, we could take all **eight bits of the third octet for the subnet.**

One drawback of subnetting is that once the subnet mask has been chosen, the number of hosts on **each subnet is fixed**. This makes it hard for network administrators to assign **IP space based on the actual number of hosts needed.**

For example, assume that a company has been **assigned 147.208.0.0 and** has decided to subnet this by using eight bits from the host portion of the address. Assume that the address allocation policy is to assign one **subnet per department in an organization**. This means that **254 addresses are assigned to each department**. Now, if one department only has **20 servers,** then **234 addresses are wasted.**

VLSM: Variable Length Subnet Masking.

- Using variable-length subnet masks (VLSM) improves on subnet masking.
- VLSM is similar to traditional fixed-length subnet masking in that it also allows a network to be subdivided into smaller pieces.
- The major difference between the two is that VLSM allows different subnets to have subnet masks of different lengths.
- For the example above, a department with 20 servers can be allocated a subnet mask of 27 bits.
- 32-27=5=$2^5 = 32$ addresses must be sufficient for this department.
- This allows the subnet to have up to 30 usable hosts on it.

CIDR: Classless Inter-Domain Routing.

- CIDR is also called super netting. It's an IP addressing scheme that replaces the older system based on classes A, B, and C.
- With CIDR, a single IP address can be used to designate many unique IP addresses.
- A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP prefix. For example: 172.200.0.0/16
- The IP prefix specifies how many addresses are covered by the CIDR address, with lower numbers covering more addresses.
- An IP prefix of /12, for example, can be used to address 1,048,576 former Class C addresses.
- For the above example, a CIDR IP prefix of /27 is sufficient for the department of 20 addresses.
- CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

The Key differences between CIDR and VLSM

- In a way there is no much difference between VLSM and CIDR, VLSM is the predecessor of CIDR which came into existence when classful networks were introduced. VLSM allows subnetting a classful network. With CIDR there are no classes and everything depends on the prefix length.
- The CIDR is the summarization of the subnets back to the classes. As against, VLSM permits you to apply variable subnet masks to the same class address space.
- CIDR uses supper netting which refers to the aggregation of the network in a single address. On the contrary, VLSM employs the concept of the subnetting which is nothing but the subdivision of one network into multiple sub addresses.

Q1.3)

Advantages of Using CIDR and VLSM together:

- Reduces the size of the routing table.
- Generates less overhead with respect to network traffic, CPU and memory.
- Provides flexibility in designing, addressing the networks.
- Effective utilization of the address space.
- It is capable of hierarchical addressing.
- Reduces the size of the routing tables.

CIDR and VLSM both allow a portion of the IP address space to be recursively divided into subsequently smaller pieces. The difference is that with VLSM, the recursion is performed on the address space previously assigned to an organization and is invisible to the global Internet. CIDR, on the other hand, permits the recursive allocation of an address block by an Internet Registry to a high-level ISP, a mid-level ISP, a low-level ISP, and a private organization's network.

Conclusion:

The CIDR allows to aggregate several networks in a single address, and this is done with the help of a routing table entry which expresses the aggregation of the network. In contrast, the VLSM helps in creating a hierarchy of subnets holding distinct sizes from an IP address space.

Question 2

Introduction

IEEE 802.11 (Institute of Electrical and Electronics Engineers) is part of the **IEEE 802 set of local area network (LAN) protocols**, that specifies the set of media access control **(MAC)** and physical layer **(PHY)** protocols for implementing wireless local area network **(WLAN)** Wi-Fi computer communication in various frequencies including, such as **2.4 GHz, 5 GHz, 6 GHz, and 60 GHz** frequency bands. Where all the standards use CSMA CD Carrier-sense multiple access with collision detection as common method.
So, IEEE 802.11 standard are divided into 9 Standards which are popularly used as of today with some of them being old.

1. IEEE 802.11 (Wireless LAN)
2. IEEE 802.11a (Wi-Fi Second Generation)
3. IEEE 802.11b (Wi-Fi First Generation)
4. IEEE 802.11g (Wi-Fi Third Generation)
5. IEEE 802.11n (Wi-Fi Fourth Generation)
6. IEEE 802.11ac (Wi-Fi Fifth Generation)
7. IEEE 802.11ad (WiGig)
8. IEEE 802.11ah (Wi-Fi HaLow)
9. IEEE 802.11ax (Wi-Fi Sixth Generation)

We will be discussing more on these IEEE 802.11 Standards in coming question.

Q-2.1)

1. IEEE 802.11a (Wi-Fi Second Generation)

802.11a was one of the first standards issued under the **802.11 Stranded in 1999.** Instead of using a 2.4 GHz band, this stranded used a 5 GHz frequency band. By using a **5 GHz frequency band this made this stranded achieve High Speeds but the Range was limited.** In order to achieve higher speeds Developers first designed **OFDM (Orthogonal Frequency Division Multiplexing) technology** it is a digital modulation method used to encode data on multiple frequencies into its coding scheme which then allows **802.11a** to have a theoretical **maximum speed of 54 Mbps,** which was a huge improvement from the original Wi-Fi standard. The Application of **802.11a was used in of most of the business networks**.

Data Rate : 1 ~ 2 Mb/s

Bandwidths : 22 MHz

Frequency Bands : 5GHz and 3.7GHz Bands were used in IEEE 802.11a

Access Techniques : OFDM (Orthogonal Frequency Division Multiplexing)**, (SISO)** Single Input Single Output.

2. IEEE 802.11b (Wi-Fi First Generation)

While **802.11 a was being developed**, Developers started to develop **802.11b alongside Second Generation Wi-Fi** and it was published in **1999. So , 802.11b** uses **DSSS (Direct-Sequence Spread Spectrum)** it is a modulation method used to reduce signal interference in the **2.4 GHz band,** allowing **802.11b** to have speeds up to **11 Mbps.** Using 2.4GHz makes this **Standard** to have more range when compared with **802.11a as we know that using a 2.4GHz** can make the data rate slower if its perks bring the range this happens when it is connected to a network interface and multiple devices are connected to it such as **Mobile Phones and Appliances etc.** The Products were cheaper when compared with 802.11a. The Main Difference with respect to products was if a product is using 802.11a adapter inside it and 802.11b cannot use that access point and vice versa.

Data Rate : 1 ~ 11 Mb/s

Bandwidths : 22 MHz

Frequency Bands : 2.4 GHz

Access Techniques : DSSS (Direct-Sequence Spread Spectrum), **(SISO)** Single Input Single Output

3. IEEE 802.11g (Wi-Fi Third Generation)

In order to fulfil the large growing demand of the **Internet.** Developers developed **802.11g and was joined the IEEE 802.11 standards in 2003.** What Developers did was they took all the best features from **First Generation and Second Generation i.e. 802.11a and 802.11b which uses 2.4GHz Band** to deliver a speed of **54 Mb/s**. Now the issue was that people still had those old access points from **First Generation and Second Generation Wi-Fi. So,** the backward compatibility was a must because many people. Now the issue was **Wi-Fi Products** only were capable of connecting to that **Access Points** under which they used to have inside them. Now let's think that a **phone** is connected to a **802.11g**
Access Point and the hardware inside that phone only supports **802.11b** Access Points now the phone couldn't use the full potential that **802.11g provides as 802.11b has maximum speed of 11 Mb/s.** But on the Other side using OFDM (Orthogonal Frequency Division Multiplexing) on **802.11a** allowed users to use its full potential as in theory it did support **54 Mb/s.**

Data Rate : 6 ~ 54 Mb/s

Bandwidths : 20 MHz and 40 MHz

Frequency Bands : 2.4GHz

Access Techniques : OFDM (Orthogonal Frequency Division Multiplexing), **DSSS (**Direct-Sequence Spread Spectrum) and **(SISO)** Single Input Single Output

4. IEEE 802.11n (Wi-Fi Fourth Generation)

In 2009 in order to improve **Speeds, Reliability, and of Range** Developers developed **IEEE 802.11n** It was the first standard to use **MIMO (Multiple-Input Multiple-Output)** technology. These Products used a series of antennas to receive more data from one device at a time which resulted in faster data transmissions. It was to first standard which allowed the usage of two radio frequencies – 2.4 GHz and 5 GHz. Now that it uses both frequencies which allowed **802.11n** to have backward compatibility with **802.11a, 802.11b and 802.11g.** With all its improved functionalities, 802.11n supported bandwidth speeds up to **150 Mb/s** and a had theoretical range of 230 ft indoors, which is a huge improvements from the previous standards.

Data Rate : Under **20MHz its 7.2 ~ 72.2 Mb/s** and Under **40MHz its 15 ~ 150 Mb/s**

Bandwidths : 20MHz and 40MHz

Frequency Bands : 2.4GHz and 5GHz Bands

Access Techniques : MIMO (Multiple-Input Multiple-Output) and **OFDM** (Orthogonal Frequency Division Multiplexing)

5. IEEE 802.11ac (Wi-Fi Fifth Generation)

The 5th generation of Wi-Fi **802.11ac** was introduced in 2013. The reason why this introduced was to reduce interference in the 2.4 GHz band, it was developed to operate under the 5 GHz band for most of the times . **802.11ac** was the first to introduce and make use of **(MU-MINO)Downlink Multi-User Multiple-Input Multiple-Output. It took Wireless-N MIMO technology** which allowed it to **take one step further to increase data transmission.** By using this **technology** it allowed wireless routers to transmit information to multiple devices at the **same time, improving bandwidth speeds and reducing latency.** As we can see now a days most of the devices use **802.11ac** standard as it allows to us to use **2.4 GHz band and 5 GHz band** just like **802.11n** but the difference were the data rates with **5 GHz band bandwidth speeds were up to 780 Mbps and using 2.4 GHz band speeds were up to 450 Mbps.**

Data Rate : Under **20MHz its 7.2 ~ 96.3 Mb/s** , at **40MHz its 15 ~ 200 Mb/s ,** at **80MHz its 32.5 ~ 433.3 Mb/s and** at **160MHz its 65 ~ 866.7 Mb/s**

Bandwidths :

Frequency Bands : 2.4GHz and 5GHz Bands

Access Techniques : (MU-MINO) Downlink Multi-User Multiple-Input Multiple-Output and **(OFDM)** (Orthogonal Frequency Division Multiplexing)

6. IEEE 802.11ax (Wi-Fi Sixth Generation)

As of **2019,** the **802.11ax standard** has become the newest Wi-Fi standard which was designed to deliver faster speeds, support more devices simultaneously, decrease latency, improve security, and increase bandwidth. To do all of this it used technologies like (**OFDMA) Orthogonal frequency-division multiple access, (MU-MINO)Downlink Multi-User Multiple-Input Multiple-Output** and (**1024-QAM) Quadrature amplitude modulation (QAM)**, and more. In theory it can output maximum speed of 10 Gb/s with all these improvements. Now **802.11ax standard** has a subcategory called **Wi-Fi 6E** which would be able to use 6GHz frequency

Data Rate : : Under **20MHz its 7.2 ~ 96.3 Mb/s** , at **40MHz its 15 ~ 200 Mb/s ,** at **80MHz its 32.5 ~ 433.3 Mb/s and** at **160MHz its 65 ~ 866.7 Mb/s**

Bandwidths : 20MHz , 40MHz , 80MHz and 160 MHz

Frequency Bands : 2.4 GHz Band , 5GHz Band and **6 GHz Band under Wi-Fi 6E**

Access Techniques : (OFDMA) Orthogonal frequency-division multiple access , **(MU-MINO)** Downlink Multi-User Multiple-Input Multiple-Output **and (1024-QAM)** Quadrature amplitude modulation**, and more.**

Conclusion

As we have seen from all the different standards uses in 802.11 Wi-Fi we have seen have a huge improvement in last 20 years or so when you compare **first generation Wi-Fi** with the **latest generation** with speeds being improved from **35 Mb/s to 10 Gb/s. B**ut still this is not the end of the Wi-Fi as developers are working on **seventh generation of Wi-Fi which is 802.11be and would be** available to consumers in 2023 and which has the **maximum speed of 40 Mb/s and supports 6 Ghz Frequency band.**

Q-2.2)

Introduction

Most of us had connected to a Wi-Fi network with our **laptop, tablet or smartphone,** and to join that network we had to select a network name and **supply a password. Supplying a password implies (better) security,** but there are different methods and protocols that are used in wireless networks to ensure security, some being less secure and some being more secure. Different Wi-Fi security protocols include **WEP, WPA, WPA2, WPA3 and WPS** are used in **802.11 Standards**.

1. WEP (Wired Equivalent Privacy)

This was the initial Encryption Protocol that was used in 801.11a and 801.11b developed in 1999 and it's the earliest security protocol that was used for wireless networks. As it is meant to deliver the **same security to wireless networks as it did for wired networks**. It is a **40-bit encryption key** that was used and it was basically vulnerable and not secure, and therefore **was easily hackable**. That's the reason why it died so early and we don't see it in today's networks as it uses **RC4 Algorithm** to generate that **40-bit encryption key**. Now let's look at how it basically encrypts the key, The algorithm operates on a user-selected variable-length key(K) of **1 to 256 bytes (8 to 2048 bits),** typically between **5 and 16 bytes.** Now the first step to is to initialize an array. It is a character array of size 256 i.e. **Encrypt [256].** After that, for every element of the array, we initialize Encrypt[i] to I,

I. **Start**
II. **Char Encrypt [256]**
III. **Initialize count = 0**
IV. **For Loop Begins where (Count < 256)**
    a. Encrypt[Count] = count
V. **Stop**

Now that we have our array we now run KSA Algorithm which will then use a secret key to scramble this array,

I. **Start**

II. Initialize **i and j**

III. **For Loop Begins where (i < 256)**

   a. j = (j + Encrypt [i] + T[i]) mod 256

   b. swap (Encrypt [i], Encrypt [j])

IV. **Stop**

Now that we scrambled our array using **KSA Algorithm** now we generate **Keystream** using **PRGA(Pseudo Random Generation Algorithm)**

I. **Start**

II. **Initialize i = j = 0**

III. **While Loop Begins**

   a. i = (i + 1) mod 256

   b. j = (j + Encrypt [i]) mod 256

   c. Swap (Encrypt [i], Encrypt [j])

   d. t = (Encrypt [i] + Encrypt [j]) mod 256

   e. k = Encrypt [t];

IV. **Stop**

This is how WEP (Wired Equivalent Privacy) works in a nutshell

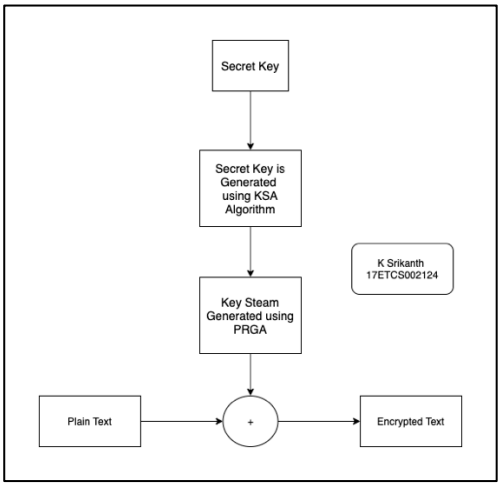

Figure 2 Flowchart of How WEP Protocol works using RC4 Algorithm for Encryption

2. WPA (Wi-Fi Protected Access) (802.11g)

After **WEP** had problems where **hackers can easily hack the network** it was outdated and moved on to **WPA (Wi-Fi Protected Access)** is another wireless security protocol that was developed to solve the problems of WEP. **WPA is far better than WEP** because it uses a stronger encryption method called **TKIP (Temporal Key Integrity Protocol).** It dynamically changes its keys as it's being used and this ensures data integrity.

TKIP is a suite of algorithms that works as a **"wrapper**" to **WEP**, which allows users of legacy **WLAN equipment to upgrade to TKIP without replacing hardware**. It uses the original **WEP programming** but "wraps" **additional code at the beginning and end to encapsulate and modify it.** Just like **WEP** this also uses the **RC4 stream encryption algorithm as its basis**. The new protocol, however, encrypts each data packet with a unique encryption key, and the keys are much stronger than those of its predecessor. To **increase key strength**, TKIP includes **four additional algorithms:**

- A cryptographic message integrity check to protect packets
- An initialization-vector sequencing mechanism that includes hashing, as opposed to WEP's plain text transmission
- A per-packet key-mixing function to increase cryptographic strength
- A re-keying mechanism to provide key generation every 10,000 packets.

Even though **WPA is more secure than WEP,** today even **WPA is outdated because TKIP did have some issues.**

3. WPA2 (2nd Generation Wi-Fi Protected Access) (802.11g, 802.11n, 802.11ac)

After **TKIP** was having some issues with its architecture then came the birth of **WPA2** that **provided even stronger security than WPA**, While WPA uses TKIP for encryption,WPA2 uses **AES (Advanced Encryption Standard)** which uses **symmetric encryption algorithm** which can resist a **brute-force attack.** So, AES includes three block ciphers **AES-128, AES-192 and AES-256.**

AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, where sa AES-192 uses a **192-bit key length** and **AES-256 uses a 256-bit key length** to encrypt and decrypt messages. There are **10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys**. A round consists of several processing steps that include **substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.**

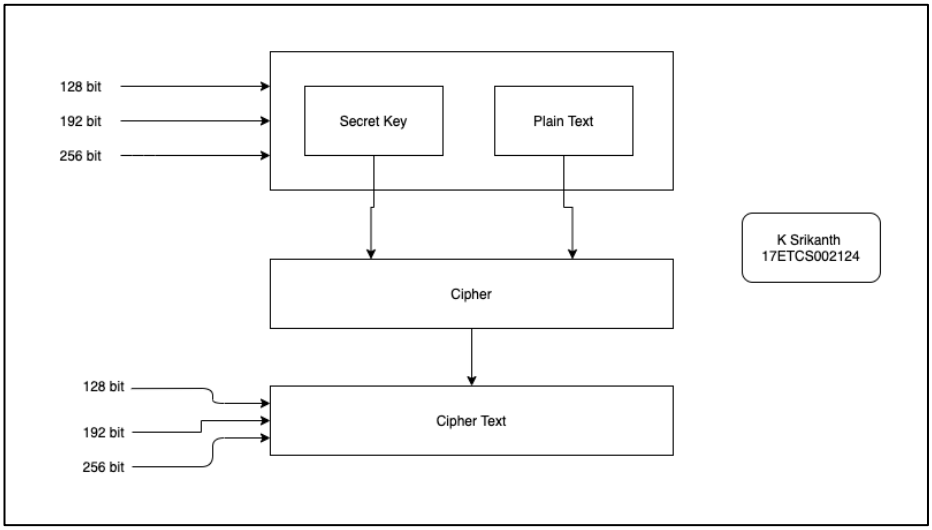

Figure 3 Flowchart of How WPA2 Protocol works using AES Algorithm for Encryption

4. WPA 3 (3nd Generation Wi-Fi Protected Access) (802.11ax)

AES still does the job as of now to protect the network but that didn't stop developers to make **WPA 3** which is **next generation of wireless security is WPA3**. This was introduced in 2018 as it provides cutting **edge security protocol which is 128-bit encryption key** and **Forward Secrecy protocol to resist offline dictionary attacks while improving key exchange security** and It adds new features to simplify Wi-Fi security and enable more standard authentication, and **provide increased protection from password guessing attempts.**