CS-B

D.C

UNIT - I

Part - A

1) Sampling theorem :-

Sampling theorem states that -

a). A bandlimited signal of finite energy which has no frequency components higher than $\omega$ hz is completely described by specifying the values of the signal at instants of time seperated by $\frac{1}{2\omega}$ sec and.

b) A bandlimited signal of finite energy which has no freq components higher than $\omega$ Hz, may be completely recovered from the knowledge of its samples taken at the rate of $2\omega$ samples per sec.

2). flat top sampling is better than natural sampling in PAM -

flat top sampling is very easy as compared to natural sampling. In flat top sampling the top of the samples remains constant and hence it is easy to reconstruct the original signal from the flat top sampled signal.

3) Aliasing effect

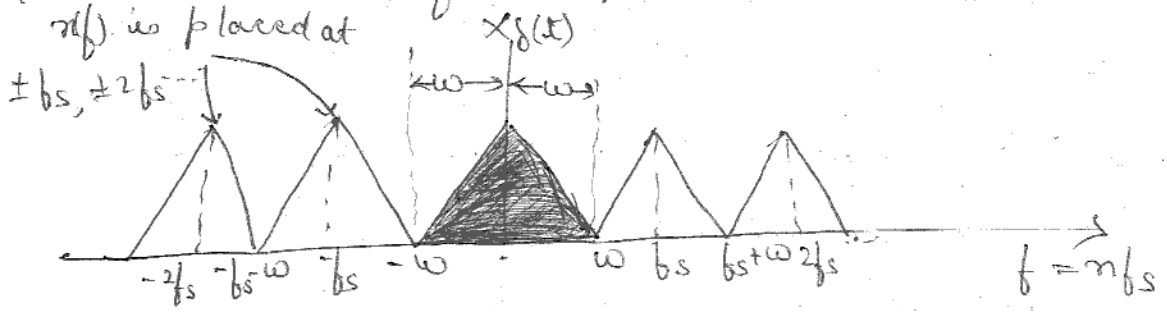
when sampling freq is less than Nyquist rate, the spectrum of the sampled signal overlaps with itself. Hence the higher frequencies take the form of lower frequencies. This interference of the frequency components is called aliasing effect.

4). Quantization :-

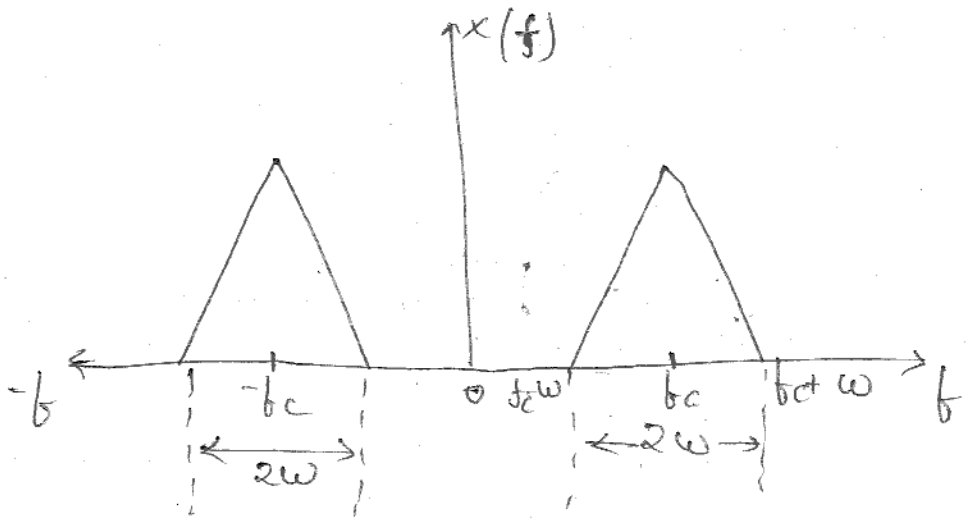
when an analog signal is converted into digital, quantization is performed. The analog value is assigned to the nearest digital level, which is called quantization. The quantization levels are fixed depending upon the number of bits.

5). Prediction filter :-

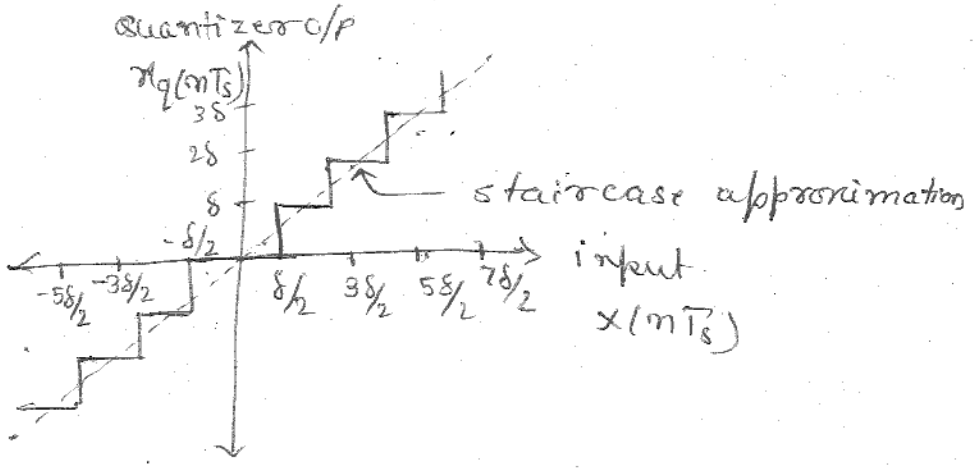
7). Spectrum of sampled low pass signal




8). Spectrum of sampled Band Pass signal



9) Mid-tread quantizer :-

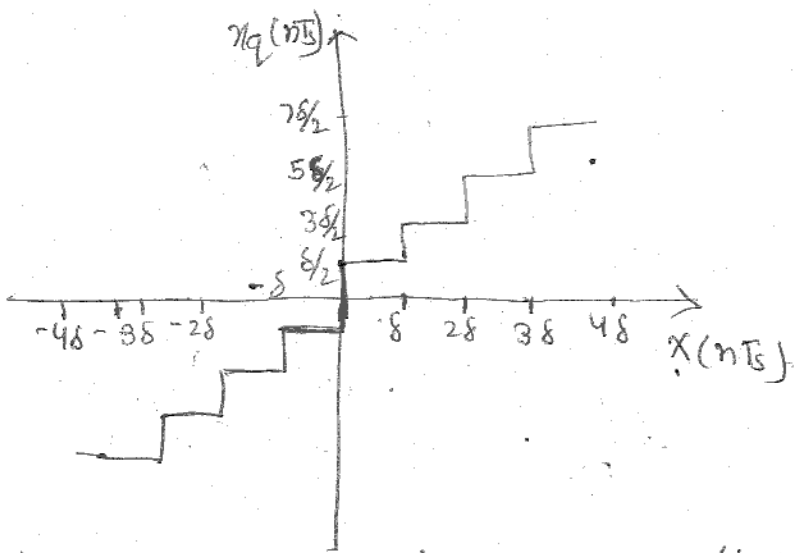



The ideal transfer characteristics in mid-tread quantizer passes through origin ie zero.

- when $x(nT_s)$ is zero the quantizer o/p is also zero, hence it called midtread quantizer.

For $-\delta/2 \leq x(nT_s) < \delta/2$ ; $x_q(nT_s) = 0$

10). Mid-riser quantizer :-




This is called midriser quantizer because its o/p is either + δ/2 or - δ/2 when i/p is zero.

for, $0 \leq x(nT_s) < \delta$ ; $x_q(nT_s) = \delta/2$

$-\delta \leq x(nT_s) < 0$ ; $x_q(nT_s) = -\delta/2$

1) quantization error :-

During quantization process, inherent errors are introduced in the signal. This error is called quantization error. It is expressed as :-

$$\mathcal{E} = x_q(nT_s) - x(nT_s)$$

Here, $x_q(nT_s)$ is quantized value of the s/l

$x(nT_s)$ is the value of sample before quantization.

2). Non-uniform quantization :-

quantization in which step size is not fixed is called non-uniform quantization. In this step size is small at low input signal levels. Hence quantization error is also small at these input. Step size is higher at high input levels. Hence S/N ratio remains almost same throughout the dynamic range of quantizer.

13). Disadvantage of uniform quantization over the non-uniform quantization — Ans. uniformmm.

13). Disadvantage of uniform quantization over the non-uniform quantization —

In uniform quantization the quantizer has a linear characteristics. The step size also remains same throughout the range of quantizer. Therefore over the complete range of I/Ps the maximum quantization error also remains same.

i.e for low signal amplitudes like 2 V or 3V and for high signal amplitudes like 15V & 16V etc. the quantization error remains same.

14) ISI :- (Intersymbol interference) :-

The transmitted waveform in PAM is represented by —

$$X(t) = \sum_{K=-\infty}^{\infty} A_K g(t - KT_b)$$

where, $A_K$ = Amplitude of $K^{th}$ pulse

$g(t)$ = Shaping Pulse

o/p at $t = iT_b$ can be expressed as :-

$$y(t_i) = \mu A_i + \mu \sum_{\substack{K=-\infty \\ K \neq i}}^{\infty} A_K \, P[(i-K)T_b]$$

where, $T_b$ = bit duration and ~~ti~~ indication.

$t_i$ = $i^{th}$ pulse.

The 2nd term in above eqn occurs due to filtering nature of the transmitter receiver and channel. The second term represents the residual effect of all other bit transmitted before and after $t_i$. This presence of o/p due to other bits interfere with the o/p of required bit. This effect is called intersymbol interference (ISI).

15). Nyquist criterion for zero ISI —

Zero ISI can be obtained if the transmitted pulse satisfies the following condition —

In time domain —

$$P[(i-K)T_b] = \begin{cases} 1 & \text{for } i = K \\ 0 & \text{for } i \neq K \end{cases}$$

Frequency domain $= \sum_{n=-\infty}^{\infty} P(f - nf_b) = T_b$

16) Eye pattern :-

It is used to study the effect of ISI in baseband transmission -

i). width of eye opening defines the interval over which the received wave can be sampled without error from ISI.

ii) The sensitivity of the system to timing error is determined by the rate of closure of the eye as the sampling time is varied.

iii) Height of the eye opening at samping time is called margin over noise.

17). Adaptive equalization :-

Adaptive equalization is used where the the transmission characteristics of the channel keep on changing. In adaptive equalization the filters adapt themselves according to the effect of the channel. i.e the coeff of the filters are changed continuously according to the received data, in such a way that the distortion in the data is reduced.

18) Nyquist interval :-

The time interval between any two adjacent samples when sampling rate is nyquist rate.

$$\text{Nyquist rate} = 2W \text{ Hz}.$$

$$\text{Nyquist interval} = \frac{1}{2W} \text{ sec}.$$

19) Nyquist rate :- when the sampling rate becomes exactly equal to 2W samples/sec for a given bandwidth of W Hz, then it is called nyquist rate.

20) Sampling theorem for band pass signal :-

The bandpass signal x(t) whose maximum bandwidth is 2W can be completely represented into and recovered from its samples. If it is sampled at the minimum rate of twice the bandwidth

# UNIT-II

## Part-A

1). Error probability of BPSK is -

$$P_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{0.6 E_b}{4 N_0}}$$

where, $E_b$ = bit energy.

$N_0$ =

$e$ = error

2). Different digital modulation technique

i) Phase shift keying (PSK)

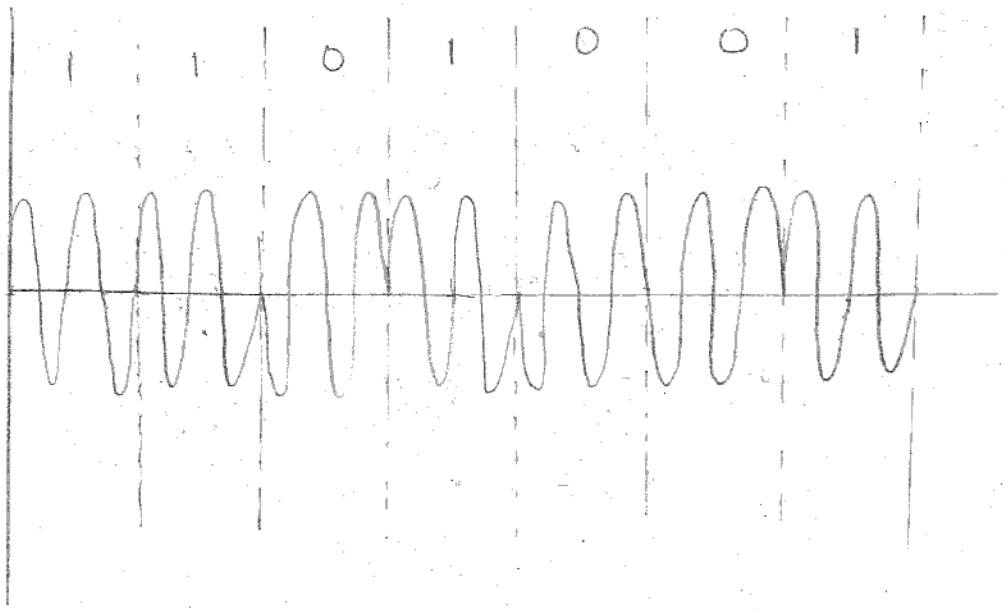
ii) Frequency shift keying (FSK)

iii) Amplitude shift keying (ASK).

3)

| BPSK | QPSK |
|---|---|
| i) Binary symbol 1 and 0 modulate the phase of the carrier | i). It has four distinct symbol and hence it is quadrature phase. |
| ii). Band width = $2f_b$ | ii) Bandwidth = $f_b$ |
| iii) Information transmission rate is lower than QPSK. | iii). Information transmission rate is heigher than BPSK. |

4). waveform of PSK for - 1101001




8).

5).

9)

8). Coherent detection :- In this method, the local carrier generated at the receiver is phase locked with the carrier at the transmitter. Hence it is also called synchron -ous detection.

Noncoherent detection :- In this method, the receiver carrier need not be phase locked with transmitter carrier. Hence it is also called envelope detection. It is simple but has higher probability of error.

9).

10) Bandwidth efficiency of M-ary PSK signal –

$$B.W = f_s - (-f_s)$$
$$= 2f_s$$
$$= 2/T_s \quad (T_s = NT_b)$$
$$=$$

11) B.W efficiency of M-ary PSK s/l –

$$B.W = 2f_s$$
$$= \frac{2}{T_s} \quad (T_s = NT_b)$$
$$= \frac{2}{NT_b}$$
$$= \frac{2f_b}{N} \quad (\because \frac{1}{T_b} = f_b).$$

B.W efficiency of M-ary FSK s/l

$$B.W = M \cdot 2f_s$$

W.K.T, $M = 2^N$ $\quad f_s = f_b/N$

$$B.W = 2 \cdot 2^N f_b/N$$
$$B.W = \frac{2^{N+1} f_b}{N}$$

12) Baseband signal receiver :-

A baseband signal receiver increases the signal to noise ratio at the instant of sampling. This reduces the probability of error. The baseband signal receiver is also called optimum receiver.

13). Matched filter :-

The matched filter is a baseband signal receiver, which works in presence of white Gaussian noise. The impulse response of the matched filter is matched to the shape of the input signal.

14). Impulse response of Matched filter :-

$$h(t) = \frac{2k}{N_0} \{x_1(T-t) - x_2(T-t)\}.$$

Here T is the period of sampling $x_1(t)$ & $x_2(t)$ are the two signals used for transmission.

15). Maximum s/n to noise ratio of the matched filter is the ratio of energy of the signal to power spectral density of white noise.

i.e $$\rho_{max} = \frac{E}{N_0/2}$$

16). The error probability of matched filter depends on energy of the signal and does not depend on shape of the signal.

$$P_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{E}{N_0}}$$

17). Correlation :-

It is the process which correlates the received noisy signal $f(t)$ with the locally generated replica of the known signal $x(t)$. Its o/p is given as:-

$$r(t) = \int_0^T f(t)\, x(t)\, dt$$

18). Binary PSK gives reduced error probability compared to ASK and FSK. It is given as :-

$$P_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{E}{N_0}}$$

19) Advantages of QPSK :-

i). For the same bit error rate, the b.w required by QPSK is reduced to half as compared to BPSK

ii) The information transmission rate of QPSK is higher.

iii). Variation in QPSK amplitude is not much, hence carrier power almost remains constant.

20). Synchronous detection :- Same as (Q - 8)

21) Envelope detection — Refer (Q-8)

22). B.W of BPSK s/d –

B.W = Highest freq – Lowest freq.

$= f_0 + f_b - (f_0 - f_b)$

$= f_0 + f_b - f_0 + f_b$

$$\boxed{B.W = 2f_b}$$

23). B.W of QPSK s/d – one bit period for two

~~B.W = 2 × 1/2T_b~~

waveforms $b_e(t)$ and $b_o(t)$ from the baseband signals is equal to $2T_b$.

$$\therefore \quad B.W = 2 \times \frac{1}{2T_b}$$

$$\boxed{B.W = f_b}$$

24). B.W of M-ary FSK.

$$B.W = M \times 2f_s$$

W.K.T $M = 2^N$

and $f_s = f_b/N$

$$B.W = 2^N \cdot 2\frac{f_b}{N}$$

$$\boxed{B.W = \frac{2^{N+1} f_b}{N}}$$

25). ON-OFF keying technique :-

It is the simplest digital modulation technique. In this, only one unit energy carrier and it is switched on or off depending upon the input binary sequence

UNIT-III

Part-A.

1). Broad types of synchronizations:-
   a) Carrier synchronization
   b) Symbol and bit "
   c) Frame "

2). Carrier synchronization:-

The carrier synchronization is required in coherent detection methods to generate a coherent reference at the receiver. Its output is frequency of phase locked loop which is used as a coherent reference s/l for detection in the receiver.

3) Two Methods for carrier synchronization
   i). Carrier Sync. using Mth power loop.
   ii) costas loop for carrier sync.

4). Symbol synchronization:-

In a matched filter the i/p signal is sampled at the end of one bit or symbol duration and the o/p is max$^m$ at $t_m = T$. Therefore the receiver has to know the instants of time at which symbol starts and when it is ended.

The estimation of these times of bit or symbol is called symbol synchronization.

5) Two methods of bit and symbol sync:-

i) closed loop bit synchronization.

ii) Early late synchronizer.

6) Disadvantages of closed loop bit sync:-

i) If there is a long string of 1's or 0's then $y(t)$ has no zero crossings and synchronization may be lost.

ii) If zero crossing of $y(t)$ are not placed at integer multiples of $T_b$ the synchronization suffers from timing jitter.

7). Frame synchronization:-

In time division multiplexing (TDM) of data, the s/l samples taken from each input channel forms a frame. The sample of one channel is called word of the frame, each word contains some fixed no. of bits. Hence the receiver has to know when a particular frame starts. This type of synchronization is called frame synchronization.

8). The signals from various sources are transmitted on the single channel by multiplexing. This requires synchronization between transmitter and receiver. For this purpose special synchronization bits are added in the transmitted signal. It is also required for detectors to recover the digital data properly from the modulated s/l.

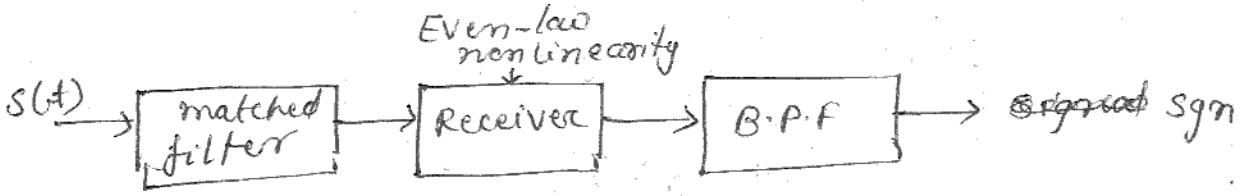
9) X. Phase locked Loop

It is the principle of phase locked loop which are the servo control loops. Their controlled parameter is the phase of a locally generated replica of the incoming carrier s/l. It has three basic components :- a phase detector, a loop filter and a voltage controlled oscillator (VCO).

10). Data aided Synchronizer :-

The synchronizing technique of Continious Phase Modulation (CPM) receiver on the basis of those that rely on knowledge of the information symbol are called data aided synchronizer.

11). Illustration of diagram of open loop bit Synchronizer




12). Bandwidth occupancy :-

The amount of bandwidth that a normalized continious phase modulated (CPM) signal will need is called Bandwidth occupancy.

13). Symbol lock :- For symbol synchronization the receiver ~~must be~~ that is able to produce a square wave that will transistion through zero as well as with the incoming signals transition between symbols is said to be in symbol lock.

9) Phase Lock :- When the receiver's local oscillator is synchronized in both frequency and phase with the received signal then it is called to be in phase lock.

14).

15] Linearized loop eq.

$$\Delta\omega(t) = \frac{d}{dt}[\hat{\theta}(t)]$$

$$= K_0 y(t)$$

$$= K_0 e(t) * f(t)$$

$$\Delta\omega(t) = K_0[\theta(t) - \hat{\theta}(t)] * f(t)$$

The linear differential eqn in $\hat{\theta}(t)$ is known as linearized loop eq.

where, $\Delta\omega(t)$ = frequency difference.

$K_0$ = gain of VCO

$f(t)$ = loop filter impulse response.

16).

(19) Steady state tracking eqn.

$$\lim_{t \to \infty} e(t) = \lim_{jw \to 0} \frac{(jw)^2 \theta(w)}{jw + K_0 F(w)}$$

(20) → (12), (21) → (16) (22) → (17)

(23) Frame marker → Frame marker is a single bit or a short pattern of bits that the transmitter injects periodically into the data stream. It is the simplest frame synchronization aid.

24). The levels of synchronization required in non-coherent modulation are:-

i) Symbol Synchronization and.

ii) Frame synchronization.

(25). CPM signaling techniques:-

1) Use signal pulses that have several orders of continuous derivatives.

2) Allow individual signal pulses to occupy multiple signal time intervals.

3) Reduce the maximum allowed phase change per symbol interval.

3)

# UNIT-IV

## Part-A

1) **Pseudo-noise (PN) sequence:-**

The sequence of noise which is added to the original or transmitted reference signal to protect it from loss or information and for security purpose is called as pseudo-noise sequence.

3) **Random Binary Sequence:-**

4) Balance Property

It is a property that can be applied to any periodic binary sequence as a test for appearance of randomness. It tells, that the no. of binary ones differs from the no. of binary zeros by at most one digit.

5) Run Property :- A run is defined as a sequence of a single type of binary digit. The alternate digit in a sequence starts a new run. The run contains ones and zeros in each period. The runs of each type are of length 1, about one-fourth are of length 2 and so on.

6) Correlation property :- According to this, if a period of the sequence is compared term by term with any cyclic shift of itself, it is best if the no. of agreements differs from the number of disagreements by not more than one count.

8) Processing gain :-

It is the measure of spread-spectrum system in the sense that, how much protection spreading can provide against against interfering signals with finite power. It is denoted as $G_P$ and given as :-

$$G_P = \frac{W_{SS}}{R}$$

$W_{SS}$ = freq bandwidth of spread-spectrum system

$R$ = chip rate.

9) Jamming effect :-

To jam a communication system in unauthorized manner by knowing all the prior system parameters, such as frequency bands, timing, traffic and so on is called jamming. The jammer use to jam the a particular communication system by choosing a jammer waveform which is accomplished at minimum cost.

10) Anti jamming :-

It is the safety of communication system against a particular threat. The fundamental ~~rule~~ ~~in~~ process of providing a jam-resistant system by making it as costly as possible for the jammer to succeed in jamming the system is called anti jamming.

12). Frequency-hop SS :-

It is a two step modulation process- data modulation and frequency-hopping modulation. The FH spectrum occupies the entire spread-spectrum bandwidth and hence it has the larger processing gain. This scheme is configured using noncoherent demodulation.

13). Slow frequency hopping :- The frequency hopping system in which there are several modulation symbols per hop is called slow frequency hopping. In this, the shortest uninterrupted waveform in the system is data symbol.

14). Fast frequency hopping :-

The frequency hopping system in which there are several frequency hops per modulation symbol. In this, the shortest uninterrupted waveform is the hop.

16) Features of code division multiple access :-

It is a
→ Allows several users to share a band of frequencies.

17). Multipath interference :-

In ~~The~~ communication system when there is more than one path from transmitter to receiver it is called multipath. It occurs due to atmospheric reflection or refraction or reflections from buildings or other objects. The multipath path wave is delayed by some time, as compared with the direct wave. Hence it interfere ~~is~~ the ~~orig~~ original s/l ~~and~~ and is called multipath interference.

18) Advantages of spread spectrum

→ ~~It uses the~~
→ The entire bandwidth of the system is used.
→ Prevent natural interference.
→ Act as resistance for noise and jamming.
→ It provides multiple access. i.e multiple user can transmit simultaneously on the same freq by using different spreading codes.

19). DSSS

i). Occupies implementable bandwidth. i.e small b.w.

ii) Processing gain is low.

iii). The occurance of error are continious and of low level.

iv) multipath degradation is low.

v) costly.

FHSS

i) occupies the entire or larger bandwidth.

ii) Processing gain is large.

iii) They suffers strong bursty errors.

iv) multipath degradation is more compared to DS.

v) cheaper than DS.

20) Acquisition :- The acquirement of a region of time and frequency uncertain in order to synchronize the received spread spectrum signal with the locally generated spreading signal is called acquisition. Usually it utilizes noncoherent detection.

21) Tracking in SS

It is the fine synchronization which is done after acquisition is completed. It is of two types coherent and noncoherent. In noncoherent, it is used to track the received PN code.

22) Applications of spread spectrum system.

→ used in the development of military guidance and communication system.
→ It is used as the jamming resistance for security purpose.
→ Used as energy density reduction.
→ high resolution ranging.
→ For multiple access. like CDMA.

23) Principle of CDMA :-

→ The code ~~divisi~~ division multiple access is based on the principle that it occupied all the bandwidth and provides multiple access, i.e it allows several users to share a band of frequencies as long as they can use different codes for their communication.

24) Types of spread spectrum :-

i) Direct sequence SS
ii) Frequency-hop SS.

25)

# UNIT :- V

## Part - A

1). unconditionally secure cipher :-

A system is said to be unconditionally secure when the amount of information available to the cryptanalyst is insufficient to determine the encryption and decryption transformations.

computational secure cipher :- ~~The~~ In this the cipher is secure for n no. of years, under circumstances favorable to the cryptanalyst the system security could be broken in a period of n years but could not be broken in less than n years.

2). Caesar cipher :- According to this, each plaintext letter is replaced with a new letter obtained by an alphabetic shift and gives the ciphertext.

eg:- plaintext :- G O T H E R E

ciphertext :- J R W K H V H

There is an alphabetic shift of 3 letters.

3. Playfair cipher :- It is a manual symmetric encryption technique. The technique encrypts pairs of letters instead of single letters as in the simple substitution cipher. The playfair is thus significantly harder to break.

4. Transposition cipher :- It is a method of encryption by which the position held by units of plaintext are shifted according to a regular system. So that the ciphertext constitutes a permutation of the plaintext. A bijective function is used on the characters, position to encrypt and an inf inverse function to decrypt.

5. Two basic function used in encryption algorithm :-
   i) substitution
   ii) Transposition

6) block cipher :- In block cipher, the plaintext is segmented into blocks of fixed size, and each block is encrypted independently from the others.

stream cipher :- It is similar to convolutional coding which have no fixed

block size.

7). Two approaches to attacking a cipher.

i) crypt analysis
ii). Brute force attack

8). diffusion :- It involves transformation that smooth out the statistical differences between characters and between character combinations.

confusion :- It involves substitutions that render the final relationship between the key ciphertext as complex as possible.

9). Purpose of S-boxes in DES :-

In cryptography an S-box is a basic component of symmetric key algorithm which performs substitution. In block cipher, they are typically used to obscure the relationship between the key and the ciphertext -

10). mono alphabetic cipher :- In this cipher our substitution character are a random permutation of 26 letters of the alphabet. For a particular alphabet only single ~~alphabet~~ substitution can be used.

10) Poly alphabetic cipher :- In this cipher the substitution rule changes continuously from letter to letter according to the element of encryption key.

11) essential ingredients of symmetric cipher.

i) Plaintext ii) Encryption algorithm.
iii) Secret key.
iv) ciphertext
v) Decryption algorithm

12) Product cipher — It is the combination of two or more transformations resulting in a cipher which is more secure than the individual components to make it resistant to cryptanalysis. The product cipher combines a sequence of simple transformation such as substitution, permutation and modular arithmetic.

13) Key expansion algorithm :-

i) The first three words are set based on constant, Sub cipher and the length of key.

ii) Each successive word is determined from the three previous words by an efficient recursive formula.

iii) The key bits are XORed into the bits of key until all the key bits were used

iv) several passes over the key table are made.

14) Triple encryption :-

The original size of DES & cipher's key size is 56 bits which is not sufficient for the increasing attacks on the security. Hence for security purpose the size of DES algorithm is increased to 3 times i.e upto 168 bit key length and is called triple encryption.

(15)

(16) Public key encryption

The public key encryption utilizes two keys one for encryption and other for decryption. In this not only encryption algorithm but also encryption key is can be publicly revealed without compromising the security of the system.

Conventional encryption :- In this a single key is used for both encryption and decryption and the encryption key can not be revealed publicly. It is shared between sender and receiver only.

17) Application of public key cryptography :-

i) . Most obvious application is its "confidentiality," the message which a sender encrypts using recipient's public key can be decrypted only by the recipient's paired public key.

ii) . Digital signature scheme, which can be used for sender authentication and non-repudiation.

iii) Used as cryptographic protocals and application in digital cash, password authenti- - cated key agreement, multi-path key agreement, etc.

18) . Message authentification :- The information that provides the verification that the message was not altered in some way is called message authentication i.e it gives the varification that the message received by the receiver is as it is that was send by sender.

20). Message Authentication Code (MAC) :-

In cryptography, a MAC is a short piece of information used to authenticate a message. A MAC algorithm is also called a keyed hash function which accepts as input a secret key and outputs a MAC. It protect the message's data integrity as well as its authenticity.

21).

II set