DC

UNIT-1

1. Sampling theorem:

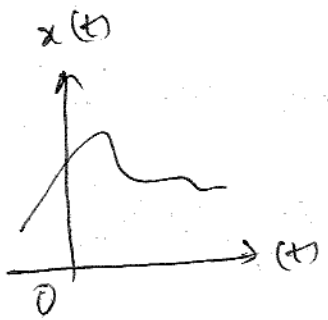
Statement:

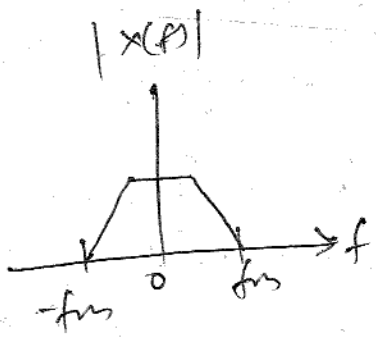
A band limited signal $x(t)$ which has the maxm frequency component 'w' and can be sampled and reconstructed back if sampling frequency f_s should be greater than and equal to twice of the maximum frequency.

ie $\boxed{f_s \geq 2w}$.

Proof:

Two parts (i) Representation of $x(t)$ sample.
(ii) Reconstruction of $x(t)$.





$$x_\delta(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT_s) \quad -(1) \qquad x_\delta(f) = \frac{1}{T_s} \sum_{n=-\infty}^{\infty} \delta(f - nf_s) \quad -(2)$$

The sampled signal $x_s(t)$ is given by

$$x_s(t) = \sum_{n=-\infty}^{\infty} x(t) \cdot x_\delta(t) \quad -(3)$$

$$x_s(t) = \sum_{n=-\infty}^{\infty} x(t) \cdot \delta(t - nT_s) \quad -(4) \qquad [\because \text{from } (1)]$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s)\, \delta(t - nT_s) \quad -(4)$$

$$x_\delta(f) = FT\left[x(nT_s)\,\delta(t-nT_s)\right]$$

$$= FT\left[\text{product of } x(nT_s) \text{ and impulse train}\right]$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s)\, e^{-j2\pi n f/f_s}$$

$$\therefore X_\delta(f) = \sum_{n=-\infty}^{\infty} x(nT_s)\, e^{-j2\pi n f T_s} \quad -(5) \quad \left[\because 1/f_s = T_s\right]$$

$$\therefore X(f) = \frac{1}{f_s} \sum_{n=-\infty}^{\infty} x(nT_s) e^{-j2\pi n f T_s}$$

$$\left[\because X_\delta(f) = f_s X(f) \;\therefore X(f) = \frac{1}{f_s} X_\delta(f)\right.$$

$$\therefore \boxed{x_\delta(t) = IFT\left[\frac{1}{f_s}\sum_{n=-\infty}^{\infty} x(nT_s)\, e^{-j2\pi n f T_s}\right]} \quad -(6)$$

ii) Reconstruction

IFT of eqn. (6) is,

$$x(t) = \int_{-\infty}^{\infty} \frac{1}{f_s} \sum_{n=-\infty}^{\infty} x(nT_s)\, e^{-j2\pi n f T_s} e^{j2\pi f t}\, df$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s) \frac{1}{f_s} \int_{-\infty}^{\infty} e^{-j2\pi n f T_s} e^{j2\pi f t}\, df$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s)\, 1/f_s \int_{-w}^{w} e^{j2\pi f (t-nT_s)}\, df$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s) \frac{1}{f_s} \left[\frac{e^{j2\pi f(t-nT_s)}}{j2\pi(t-nT_s)}\right]_{-w}^{w}$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s) \frac{1}{f_s} \left\{\frac{e^{j2\pi w(t-nT_s)} - e^{-j2\pi w(t-nT_s)}}{j2\pi(t-nT_s)}\right\}$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s) \frac{1}{f_s} \left[\frac{\sin 2\pi W(t-nT_s)}{\pi(t-nT_s)} \right]$$

$$x(t) = \sum_{n=-\infty}^{\infty} x(nT_s) \left[\frac{\sin 2\pi W(t-nT_s)}{\pi(f_s t - f_s n T_s)} \right] - (2)$$

Here, $f_s = 2W$

$\therefore T_s = \frac{1}{f_s} = \frac{1}{2W}$

$$\therefore x(t) = \sum_{n=-\infty}^{\infty} x(nT_s) \frac{\sin\pi\left(t - n\frac{1}{2W}\right)}{\pi(2Wt - n)}$$

$$= \sum_{n=-\infty}^{\infty} x(nT_s) \frac{\sin\pi(2Wt - n)}{\pi(2Wt - n)}$$

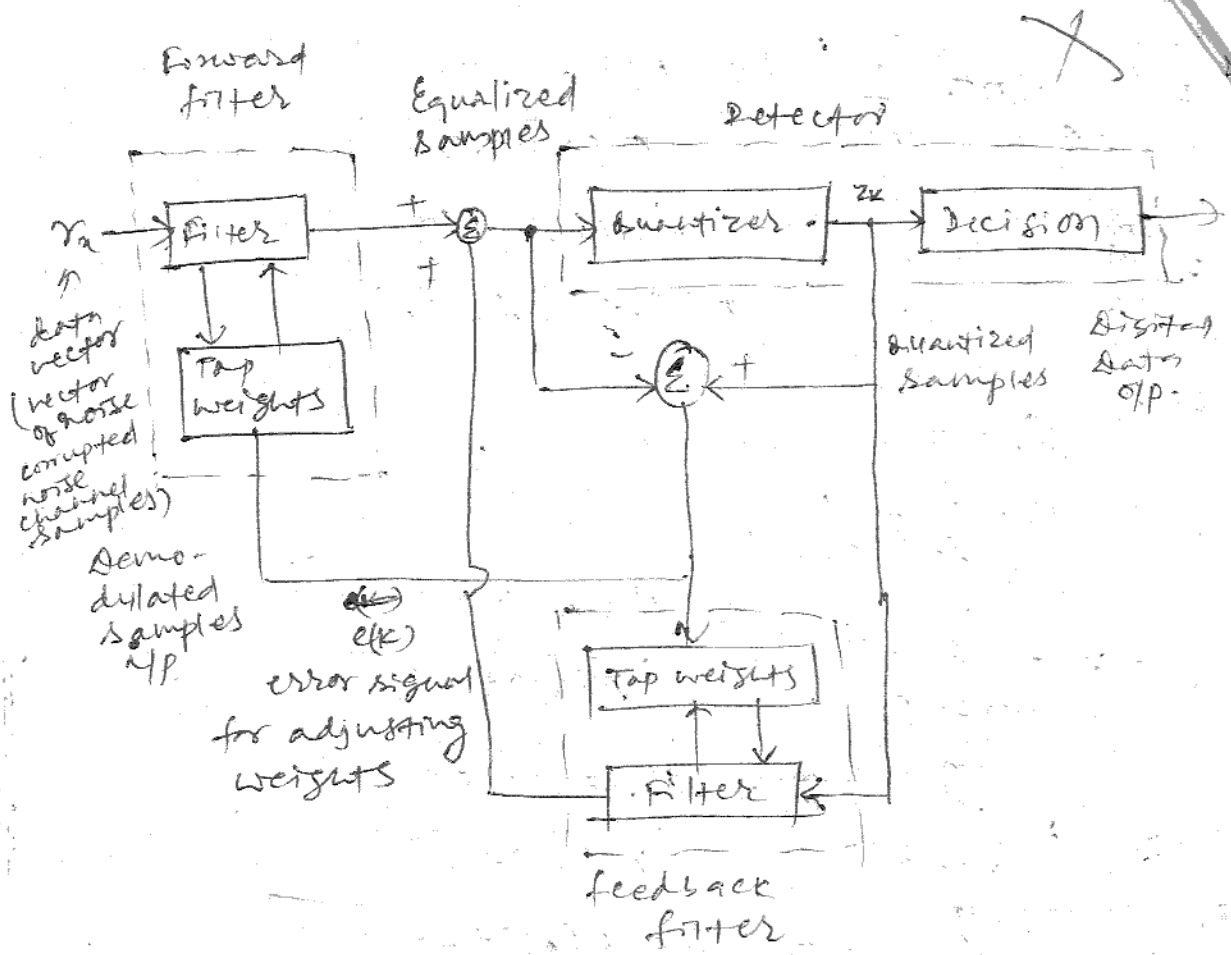
$$\boxed{x(t) = \sum_{n=-\infty}^{\infty} x(nT_s) \, \mathrm{sinc}(2Wt - n)}$$

$\left[\because \frac{\sin\pi\theta}{\pi\theta} = \mathrm{sinc}\theta \right]$

where, sinc is the interpolating function.

2] Structure of an adaptive equalization for data transmission.

The equalization which has a capable of tracking a slowly time-varying channel response is known as adaptive equalization.



- If the weights remain fixed during transmission of data, the equalization is called preset equalization.
- It can be implemented to perform tap weight adjustments periodically or continually.
- periodic adjustments are accomplished by periodically transmitting a preamble sequence of digital data is known as advance by the receiver.
- The receiver also uses to detect the start of transmission, to set the AGC level and to align internal clocks and local oscillator with the received signal.

en performed continually and automatically, the adaptive procedure is referred to as decision directed.

- Decision directed only addresses how filter tap weights are adjusted i.e. with the help of a signal from the detector.
- There exists an additional filter that operates on the detector o/p and recursively feeds back a signal to detector i/p.
- Thus, with DFE, there are two filters, a feedforward feed-forward filter and a feedback ~~fee~~ filter that process the data. and help ~~the~~ mitigate the ISI.
- decision-directed adaptive equalization successfully cancels ISI when the initial probability of error due to probability of error exceeds one percent.
- If the probability error exceeds one percent, the decision directed ~~equi~~ equalizer might not converge.

$$e(k) = z(k) - \hat{z}(k) \quad \text{— (1)}$$

- $e(k)$: error
- $z(k)$: desired o/p signal. (a sample free of ISI)
- $\hat{z}(k)$: filter o/p signal

The set of weights at each time k as

$$c(k+1) = c(k) + \Delta e(k) r_k \quad \text{— (2)}$$

- $c(k)$: vector of filter weights at time k
- Δ: controls the rate of convergence

- when the receiver is implemented in quadrature fashion, such that the signals appear as real

3] ~~Tapped delay line filters~~

2] Adaptive Equalization

It is used to keep varying the characteristics of channel.

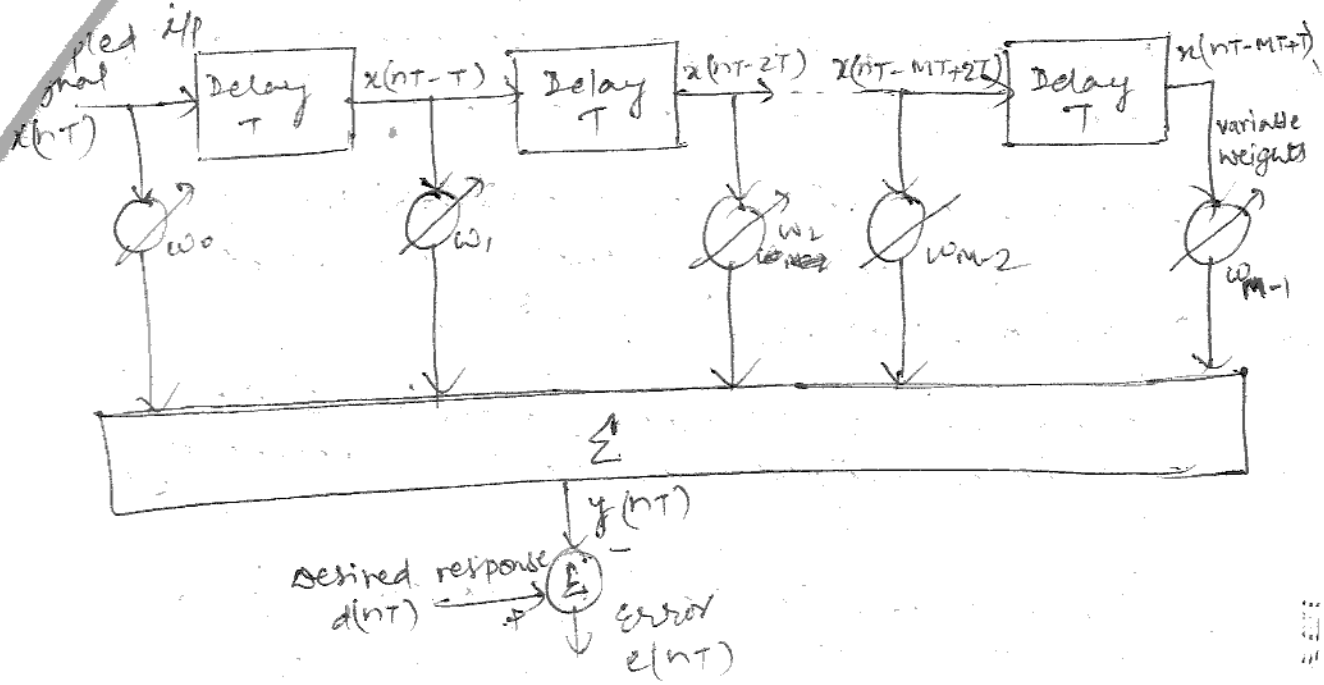
Basic principle :

In adaptive equalization, the filters adapt themselves to the dispersive effects of the channel. ie. the coefficients of the filters are changed continuously according to the received data, The filter coefficients are changed in such a way that the distortion in data is reduced.

Types

i) ~~but~~ when an equalization is done at the transmitting side, it is called prechannel equalization. It requires a f/b to know the amount of distortion in the received data.

ii) when the equalization is done at the receiving side, it is called post channel equalization. In this case, no f/b is required. The equalizer is placed after the receiving filter in the receiver.



Structure of adaptive equalizer

- The adaptive equalizer shown in fig. above is a tapped-delay-line filter. It consists of set of delay elements and variable multipliers

- The sequence $x(nT)$ is applied to the input of adaptive filter.

- The o/p $y(nT)$ of the adaptive filter will be,

$$y(nT) = \sum_{i=0}^{M} w_i x(nT-iT) \quad \text{——— (1)}$$

- The weights w_i on the taps are adaptive filter coefficients. A known sequence $\{d(nT)\}$ is transmitted first. This sequence is known to the receiver.

Error sequence b/w two sequences is,

$$e(nT) = d(nT) - y(nT) \quad n = 0, 1, \ldots N-1 \quad \text{— (2)}$$

- If there is no distortion in the channel then $d(nT)$ and $y(nT)$ will be exactly same, producing zero error sequence.
- Then the weights of the filter i.e w_i are changed recursively such that error $e(nT)$ is minimized.
- There are standard algorithms to change weights of the filter recursively.

Least Mean Square (LMS) Algorithm:

- to change the tap weights of the adaptive filter recursively.

The tap weights are adapted by this algorithm as follow:

$$\hat{w}_i(nT+T) = \hat{w}_i(nT) + \mu\, e(nT)\, x(nT - iT) \quad \text{--- (2)}$$

Here, $i = 0, 1, \ldots M-1$

$\hat{w}_i(nT)$ = present estimate for tap 'i' at time nT.

$\hat{w}_i(nT+T)$ = updated " " " " " "

μ = adaption constant.

$x(nT-iT)$ → filtered input

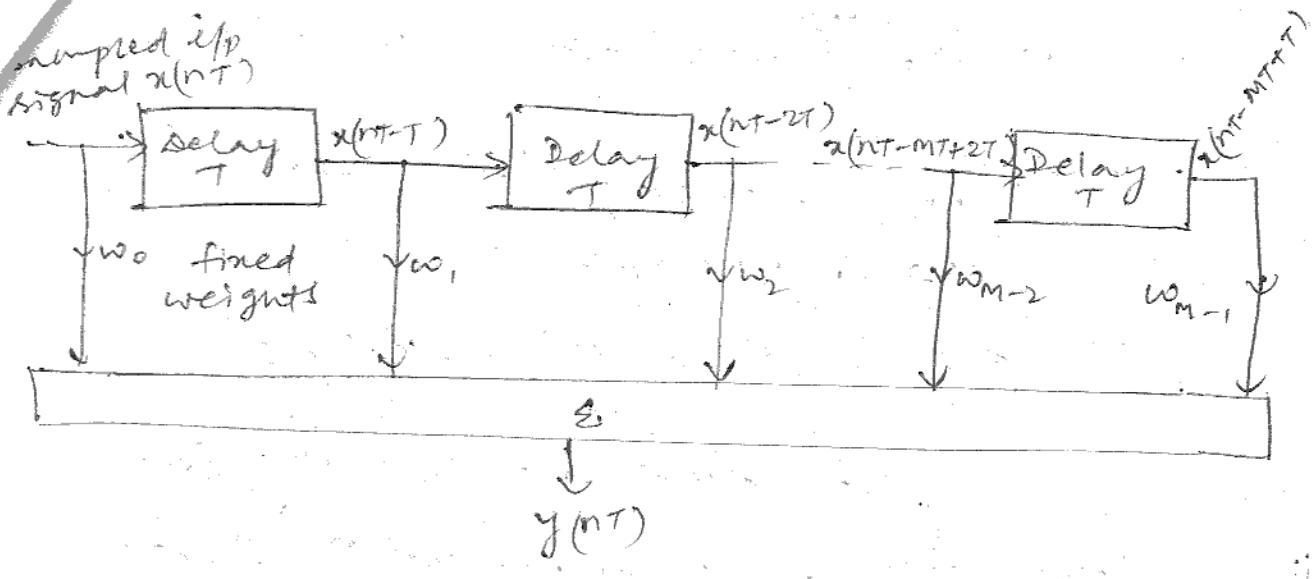
$e(nT)$ → error signal.

μ → controls the amount of correction applied to the old estimate to produce updated estimate

with the help of eqn (2) the tap weights are obtained in recursive manner.

- In this algorithm, initial tap weights are assumed zero.

Tapped Delay Line filters



Tapped delay line filter.

- A tapped delay line is a delay line which provides access to its contents at arbitrary intermediate delay length values.
- In general, a tap delay line is implemented as a single buffer in memory.
- Tap delay lines can be interpolating or non-interpolating.
- It can efficiently model multiple echoes from the same sound source & are useful in artificial reverberation.

The o/p of above filter is,

$$y(nT) = \sum_{i=0}^{M-1} w_i \, x(nT - iT) \quad -(1)$$

where, w_i is the weight of i^{th} tap

$M \Rightarrow$ total no of taps

$T \Rightarrow$ Symbol duration of the signal.

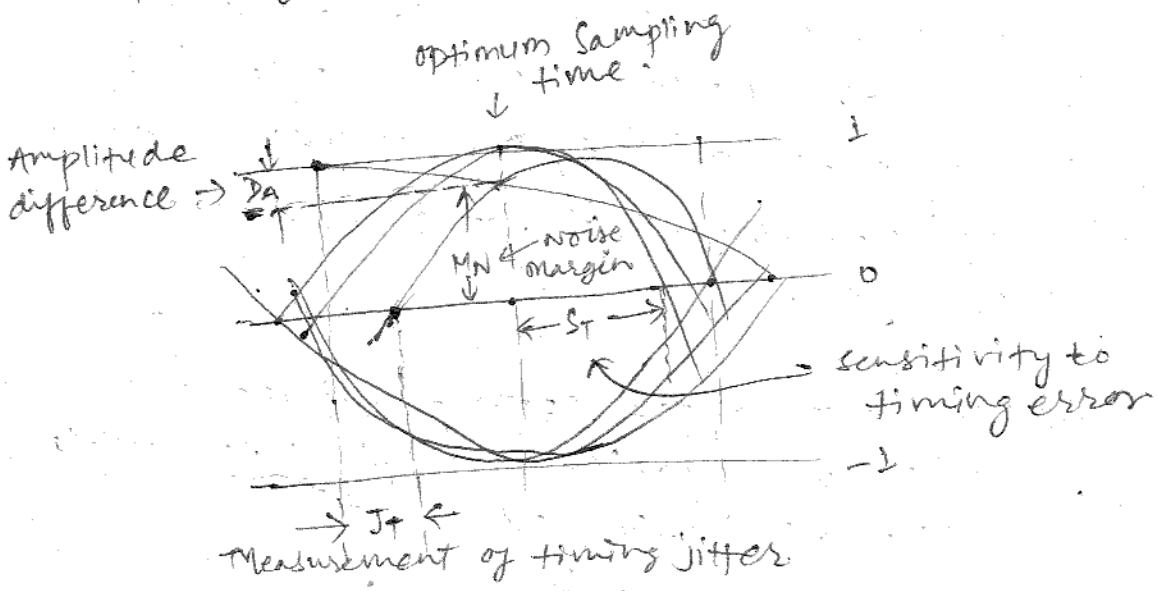
The weights are basically filter coefficicients. The approximation will be more accurate if we use more taps in the filter.

The weights are calculated once as per the characteristics of channel. Hence, this is fixed filter.

- It is explained that a correlated tapped delay line model needs to be assumed for transmission performance estimation using Rake combining even though the propagation channel itself can be characterized as a wide sense stationary uncorrelated scattering channel.

formation and application of eye pattern with relevant diagram for a stream of bits.

- An eye pattern is the display that results from measuring a system's response to baseband signals in a prescribed way.
- Eye diagram is the data transition of the digital signal for testing wheather the device is pass the protocal or not. It is for testing the falling / rising time / hold time of the device.
- Eye diagram is an oscilloscope display in which a digital data signal from a receiver is repetitively sampled and applied to the vertical input, while the data rate is used to trigger the horizontal sweep. It is so called because, for several types of coding, the pattern looks like a series of eyes between a pair of rails.



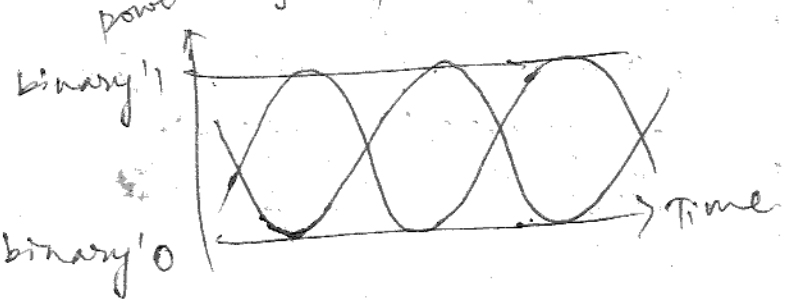


Fig Graphical eye pattern.

- on the vertical plates of an oscilloscope, we connect the receiver's response to a random pulse sequence.
- on the horizontal plates, we connect a sawtooth wave at the signaling frequency.
- In other words, the horizontal time base of the oscilloscope is set equal to the symbol (pulse) duration.

- This setup superimposes the waveform in each signaling interval into a family of traces in a single interval (0,T) as in above fig.

- The above fig. illustrates the eye pattern that results for binary bipolar pulse signaling.
- It is so because the symbols stem from a random source, they are sometimes +ve and sometimes -ve and the persistence of the cathode ray tube displays allows us to see the resulting pattern shaped as an eye.

- The width of the opening indicates the time, over which sampling for detection might be performed.

- The optimum sampling time corresponds to the maximum eye opening, yielding the greatest protection against noise.

If there were no filtering in the system i.e. if the B.W corresponding to the transmission of these data pulses were infinite then the system ~~responsed~~ responds rectangular pulse shapes.

- In that case the pattern would look like a box rather than an eye.

- The range of amplitude difference (D_A) is a measure of distortion caused by ISI, and the range of time differences of the zero crossings labelled J_T is a measurement of the timing jitter.

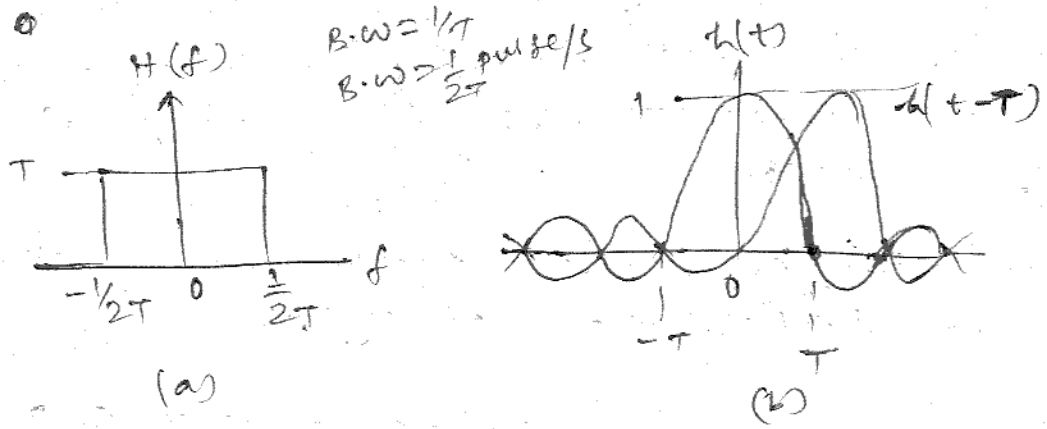
- Measures of noise margin (M_N) and sensitivity to timing error ST are shown.

Applications

i) Used to measure the effects of ISI on random data being transmitted through a particular media.
As the eye closes, ISI increases.
" " " opens; " decreases.

ii) Used to measure the amount of jitter versus the ISI.

5] a] Spectral Diagram of ideal Nyquist C



(a) (b)

Nyquist Channel for zero ISI
a) Rectangular system transf. function H(f)
b) Received pulse shape $h(t) = \text{sinc}(t/T)$.

- The theoretical minm system bandwidth needed in order to detect ~~Rs/2~~ Rs symbols/s without ISI, is Rs/2 hertz.

- This occurs when the system transfer function H(f) is made rectangular, as shown in fig (a).

- For baseband systems, when H(f) is such a filter with single sided bandwidth $\frac{1}{2T}$ (the ideal Nyquist filter) its impulse response, the inverse fourier transform of H(f) is of the form of
$h(t) = \text{sinc}(t/T)$.

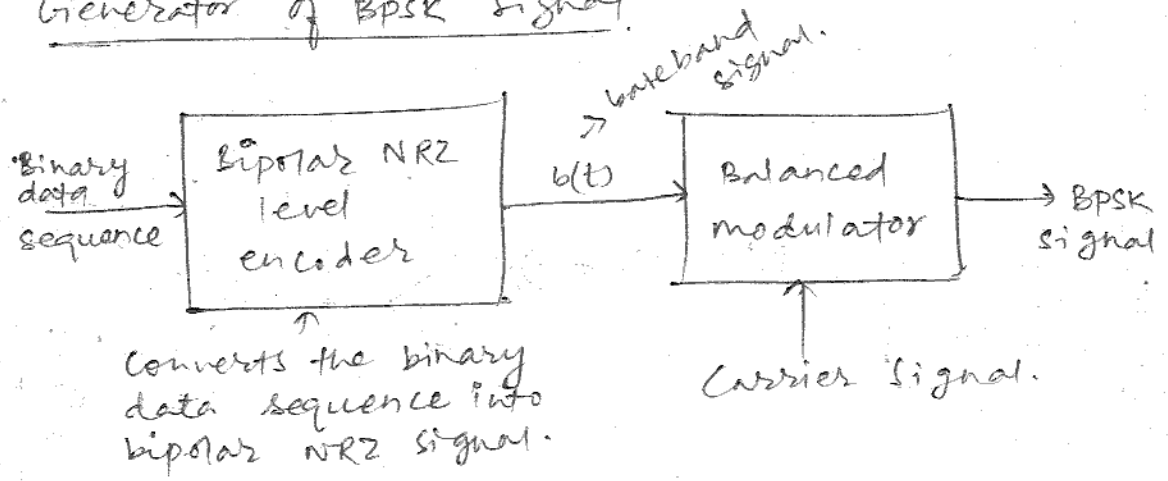
- $\text{Sinc}(t/T)$ - shaped pulse is called the ideal Nyquist pulse.

- Nyquist established that if each pulse of a received sequence is of the form $\text{Sinc}(t/T)$, the pulses can be detected without ISI.

UNIT-II

4] (a) Generation & Reception of BPSK

Generator of BPSK signal



BPSK generation scheme.

- BPSK signal can be generated by applying carrier signal to the balanced modulator.
- The baseband signal b(t) is applied as a modulating signal to the balanced modulator.
- The NRZ level encoder converts the binary data sequence into bipolar NRZ signal.

Reception of BPSK signal

The transmitted BPSK signal is

$$s(t) = b(t)\sqrt{2P}\cos(2\pi f_0 t) \quad \text{— (1)}$$

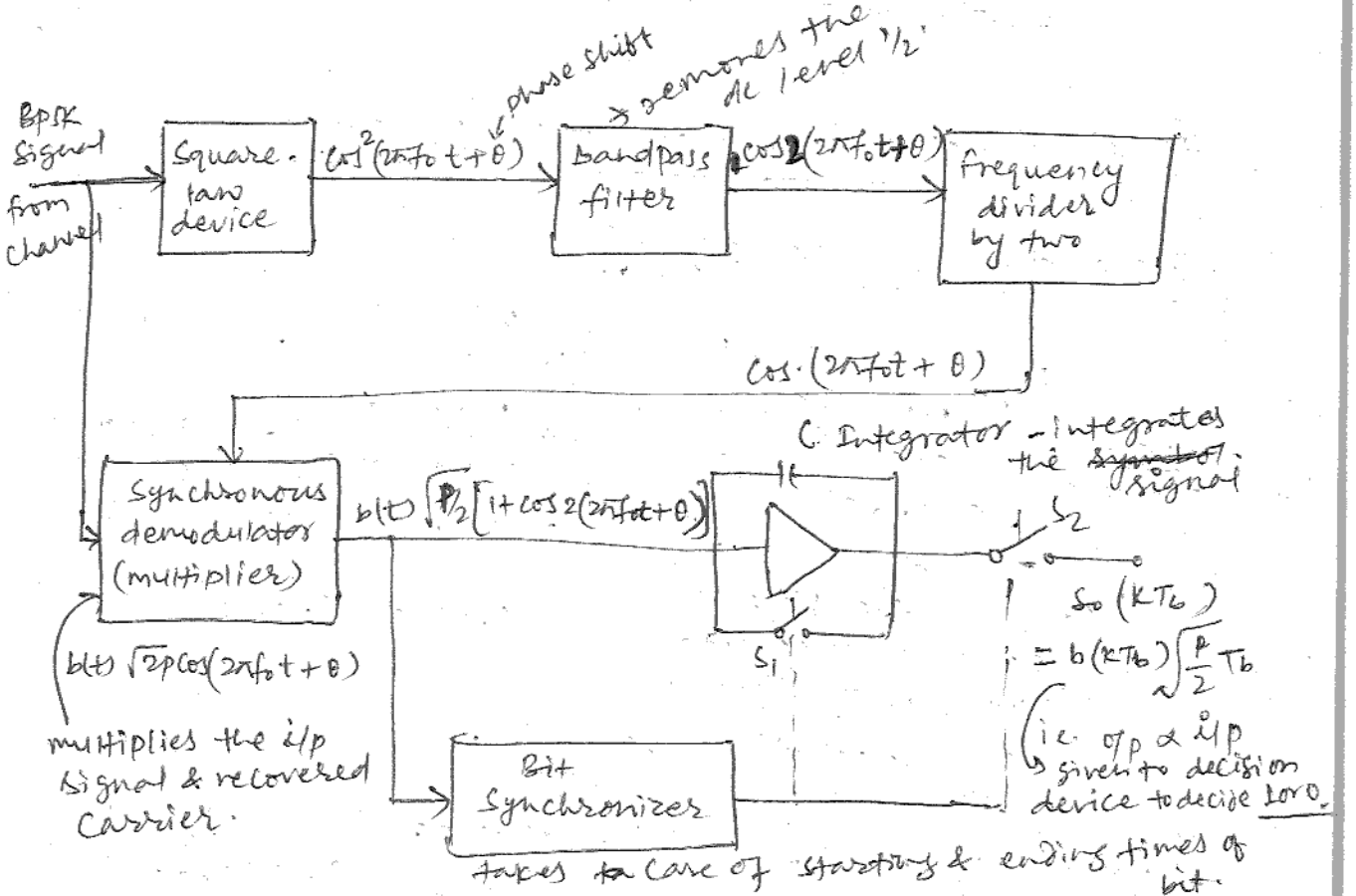


fig. Reception BPSK scheme

- $S(t)$ undergoes the phase change depending upon the time delay from transmitter to receiver. Normally, it is fixed i.e

$$S(t) = b(t)\sqrt{2P}\cos(2\pi f_0 t+\theta) \quad -(1)$$

Square law device: Here, a carrier is separated since, this is coherent detection. The received signal is passed through it. At o/p, the signal will be,

$$\cos^2(2\pi f_0 t+\theta) \quad -(2)$$

Amplitude is neglected.

$$\cos 2\theta = \frac{1+\cos 2\theta}{2}$$

$$\cos^2(2\pi f_0 t+\theta) = \frac{1+\cos 2(2\pi f_0 t+\theta)}{2}$$

$$= \tfrac{1}{2} + \tfrac{1}{2}\cos 2(2\pi f_0 t+\theta)$$

$\frac{1}{2}$ represents a DC level.

b) probability of error equation for BPSK

- The probability of detector making an incorrect decision is termed as the probability of symbol error (P_E).

- It is often convenient to specify system performance by the probability of bit error (P_B), even when decisions are made on the basis of symbols for which $m > 2$

- for this case, the symbol error probability is the bit error probability.

Assume that signal $s_i(t)$ $(i = 1, 2)$ is transmitted, the received signal $r(t)$ is equal to $s_i(t) + n(t)$, where,

$n(t) \rightarrow$ is an AWGN process, and any degradation effects due to channel-induced ISI or circuit-induced ISI have been neglected.

Two types of errors can be made:

i) If the signal $s_1(t)$ is transmitted but the noise is such that the detector measures a negative value for $z(t)$ & chooses hypothesis H_2, the hypothesis that $s_2(t)$ was sent.

ii) If signal $s_2(t)$ is transmitted but the ~~noise is such that~~ detector measures a positive value for for $z(T)$ and chooses hypothesis H_1, the hypothesis that the signal $s_1(t)$ was sent.

$s_1(t)$ if $z(T) > Y_0 = 0$

$s_2(t)$ otherwise.

The eqn for the probability of a bit error P_B, for the binary minimum error detector can be written as,

$$P_B = \int_{\frac{(a_1-a_2)}{2\sigma_0}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right) du \quad -(*)$$

$$= Q\left(\frac{a_1-a_2}{2\sigma_0}\right) \quad -(1)$$

where,

σ_0 → standard deviation of the noise out of the correlator.

$Q(x)$ → complementary error function or co-error function, which is defined as,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{u^2}{2}\right) du \quad -(2)$$

In BPSK, for equal energy antipodal signaling, the receiver o/p signal components are

$a_1 = \sqrt{E_b}$ when $S_1(t)$ is sent

$a_2 = -\sqrt{E_b}$ " $S_2(t)$ " "

where, E_b is the signal energy per binary symbol.

For AWGN, replace σ_0^2 by $N_0/2$.

So, eqn (*) becomes,

$$P_B = \int_{\sqrt{2E_b/N_0}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right) du \quad -(3)$$

$$\boxed{P_B = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)} \quad -(4)$$

(5) Probability of error eqn for BPSK

We know, The ~~general~~ probability of bit error for coherent antipodal signals are

$$P_B = \int_{\sqrt{2E_b/N_0}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-u^2}{2}\right) du \quad - (1)$$

$$P_B = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad - (2)$$

A more general treatment for binary coherent signals give the following eqn for P_B

$$P_B = \frac{1}{\sqrt{2\pi}} \int_{\sqrt{(1-\rho)E_b/N_0}}^{\infty} \exp\left(-\frac{u^2}{2}\right) du \quad - (3)$$

where, $\rho = \cos\theta$ is the time cross-~~relation~~ correlation coefficient between signal $s_1(t)$ and $s_2(t)$, where θ is the angle between signal vectors s_1 and s_2.

For antipodal signals such as BPSK,

$\theta = \pi$, thus $\rho = -1$.

For orthogonal signals such as binary FSK, $\theta = \pi/2$, since the s_1 and s_2 vectors are perpendicular to eachother. Thus, $\rho = 0$ as can be verified from eqn (3)

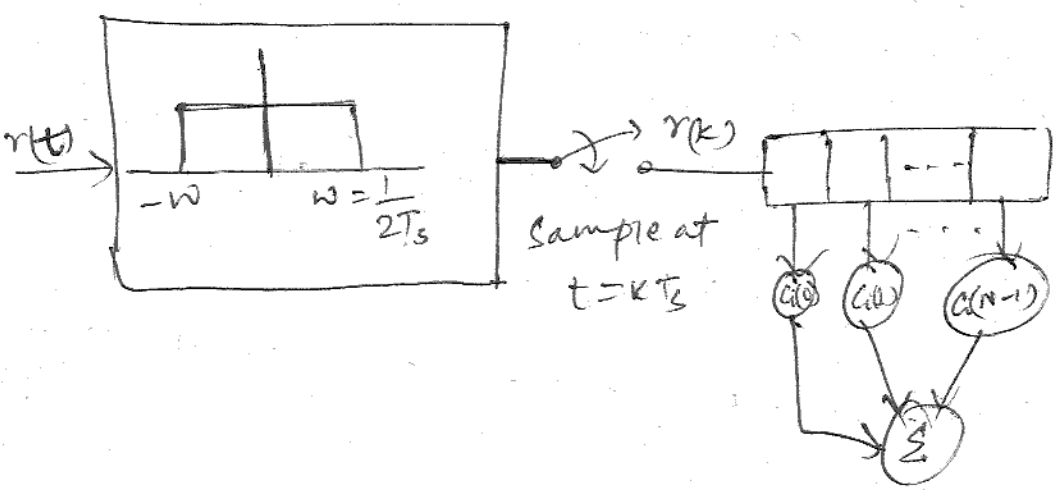
$$P_B = \frac{1}{\sqrt{2\pi}} \int_{\sqrt{E_b/N_0}}^{\infty} \exp\left(\frac{-u^2}{2}\right) du = Q\left(\frac{E_b}{N_0}\right) \quad - (4)$$

If we compare eqns (3) & (4), we can say that 3-dB more E_b/N_0 is req^d for BFSK to provide the same performance as BPSK.

BFSK is signaling 3-dB worse than BPSK signaling, since for a given signal power, the distance squared b/w orthogonal vectors is a factor of two less than the distance ~~req^d~~ squared b/w ~~theirs~~ antipodal vectors.

(6) performance of matched filter by obtaining error probability

- Matched filter is an ideal filter which processes a received signal to minimize the effect of noise. Hence, it maximizes the signal to Noise ratio (SNR) of the filtered signal.



$$z(k) = \sum_{n=0}^{N-1} r(k-n)\, c_i(n)$$

Fig. Sampled matched filter.

The matched filter is linear filter, h, that maximizes the o/p SNR.

$$z(k) = \sum_{n=0}^{N-1} r(k-n)\, c_i(n) \quad \text{— (1)}$$

~~Though we~~ we can derive the linear filter that maximizes o/p SNR by invoking a geometric argument.

(4) Timing Synchronization.

- we need the time synchronization algorithm to be scalable with the no. of nodes being deployed.

- Moreover, the time synchronization requirements are much more limiting effect, often requiring synchronization of the order of micro seconds among nodes involved in a task such as tracking a target.

- Timing synchronization is achieved by stations periodically exchanging timing information through beacon frames.

- Each station is an Independent Basic service set (IBSS) shall adopt a received timing if it is later than the station's.

- one of the principle design guidelines for our time synchronization approach is that it should be multi-modal.

- The wide range of requirements across application cannot be satisfied by a single scheme - as no single scheme is optimal along all axes.

Eg. Gps time is an attractive form of time synchronization

Drawbacks

- It has drawbacks:
  - It is not ~~ever~~ available ~~ubiquitously~~ ubiquitously & requires a relatively high-power receiver that is not feasible on the smallest, cheapest nodes.

Carrier Synchronization

- In a radio receiver, the generation of a reference carrier with a phase closely matching that of a received signal.

- In autonomous radio operation, the most optimistic situation would be that the receiver contain a carrier synchronization structure i.e. capable of track a QPSK modulation.

- Each carrier synchronization loop developed for a given modulation format, constellation and, data rate/type has certain unique characteristics.

Carrier Synchronization in BPSK.

Both the carriers are to be synchronized properly in coherent detection in BPSK.

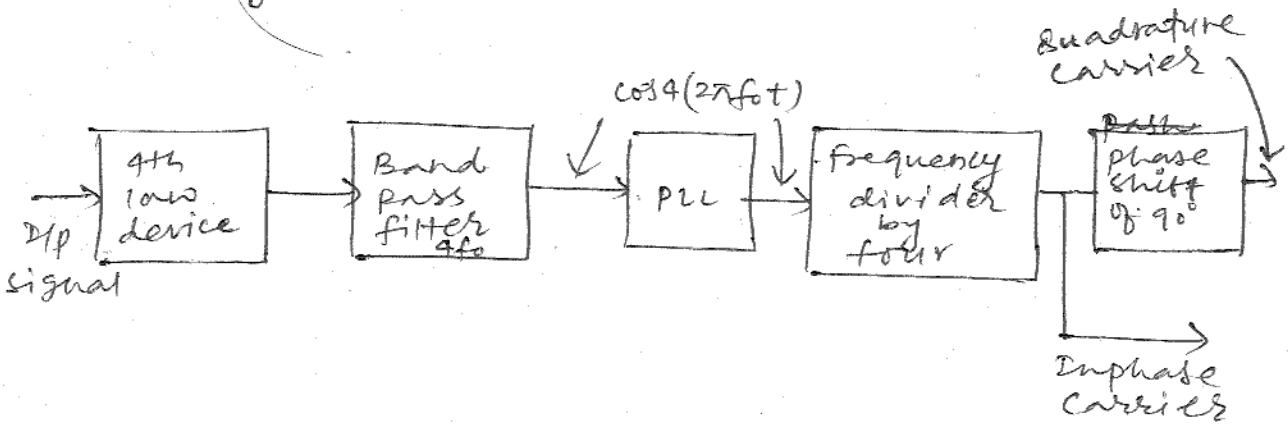


Fig. PLL system for Carrier synchronization

- The fourth power of the i/p signal contains discrete frequency component at $4f_0$.

we know that,

$$\cos 4(2\pi f_0 t) = \cos(8\pi f_0 t + 2\pi N) \quad -(1)$$

where, N → No. of cycles over the bit period which is always an integer value

- when the frequency division by 4 takes place, the RHS of above eqn (1) becomes,

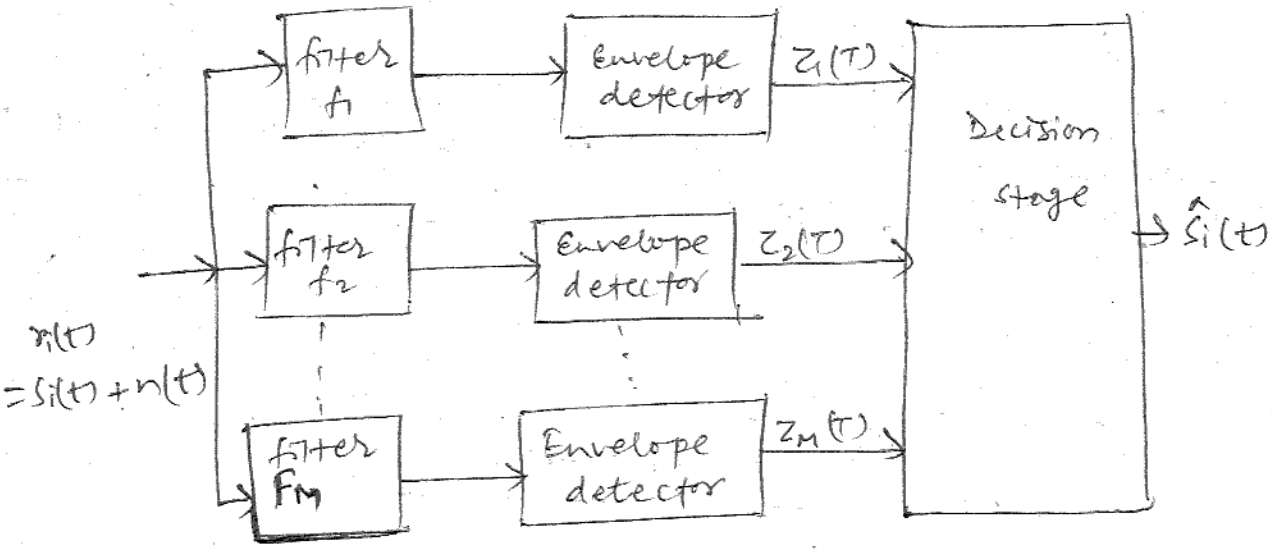
$$\cos\left(2\pi f_0 t + \frac{N\pi}{2}\right)$$

which shows that the o/p has fixed phase error of $N\pi/2$.

- Differential encoding may be used to nullify the phase error events. The PLL remains locked with the phase of '$4f_0$' & then o/p of PLL is divided by 4, which gives a coherent carrier.
- A 90° phase shift is added to this carrier to generate a quadrature carrier.

8] a) Non-Coherent BFSK Modulation

Bandpass filters centered at f_i with B.W $w_f = 1/T$, $f_i = w_i/2\pi$



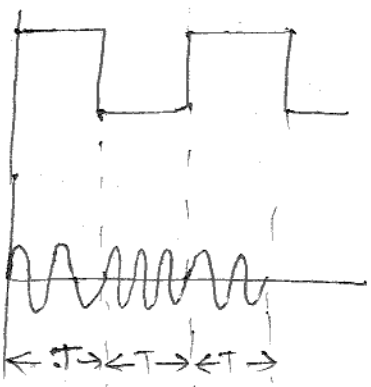
filter the frequencies from a wide range of mixed signals.

Fig. Non-Coherent detection of FSK using envelope detectors.

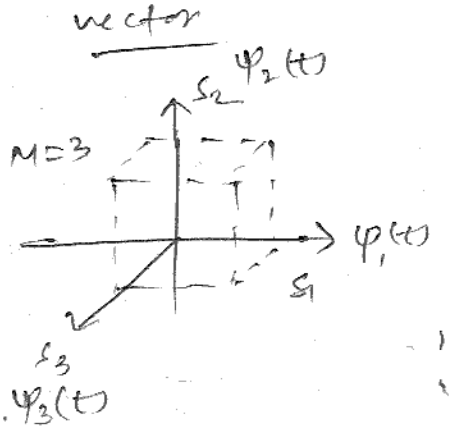
- An envelope detector consists of a rectifier and a low pass filter.
- The detectors are matched to the signal envelopes and not to the signal themselves.
- In Case of binary FSK, the decision of transmitted one or zero is made on the basis of which of two envelope detectors has the largest amplitude at the moment of measurement.
- In this case, the amplitude and the phase of the i/p signal are constant where frequency is varied.

- Now, the decision stage at the receiver revealed the information carried by the value zero or one as an output.

waveforms.



vector



$$s_i(t) = \sqrt{\frac{2E}{T}} \cos(\omega_i t + \phi)$$

ϕ ← arbitrary constant.

$\omega_i t$ has M discrete values.

$i = 1, 2, \ldots M$

$0 \le t \le T$

b) probability of error eqn for BFSK Modulation

Let us consider ~~BFS~~ non-Coherent BFSK modulated signal as follows:

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos(\omega_i(t) + \phi) \quad -① \qquad 0 \le t \le T,\ i = 1,2$$

where,
the phase term ϕ is unknown and assumed constant.

- The detector is characterized by $M = 2$ - channels of bandpass filters and envelope detectors.

The received signal

$$x(t) = s_i(t) + n(t),$$

where, $n(t)$ → white Gaussian noise process with two-sided power spectral density $N_0/2$.

Assume that, $s_1(t)$ and $s_2(t)$ are separated in frequency.

The eqn of probability error is.

$$P_B = \frac{1}{2} \exp\left(-\frac{A^2}{4\sigma_0^2}\right) \quad \text{——} ②$$

where, $A = \sqrt{\frac{2E}{T}}$

we can express the filter o/p noise as $\sigma_0^2 = 2\left(\frac{N_0}{2}\right) w_f$ —— ③

where, $G_n(f) = N_0/2$ and

$W_f \rightarrow$ filter bandwidth.

Thus, the eqn becomes,

$$P_B = \frac{1}{2} \exp\left(\frac{-A^2}{4 N_0 W_f}\right) \quad \text{---} (4)$$

$P_B \propto$ Bandpass filter B.W & that $P_B \downarrow$ as $W_f \downarrow$.

The result is valid only when ISI is negligible.

$$P_B = \frac{1}{2} \exp\left(\frac{-A^2 T}{4 N_0}\right) \quad \text{---} (5)$$

$$= 1/2 \exp\left(\frac{-E_b}{2 N_0}\right) \quad \text{---} (6)$$

where $E_b = (1/2) A^2 T$ is the energy / bit

P_B, non coherent FSK requires approx 1 dB more E_b/N_0 than that for coherent FSK (for $P_B \leq 10^{-4}$).

- Non-coherent receiver is easier to implement, because coherent reference signals need not be generated.

∴ Almost, all FSK receivers use non-coherent detection.

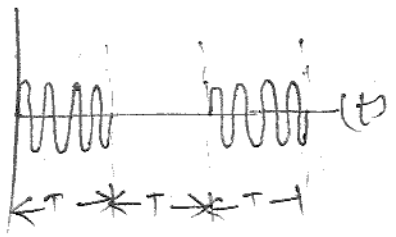
10). (a) ASK. (ON-OFF keying)

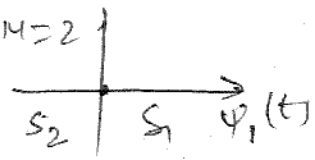
analytic waveform vector.

$$s_i(t) = \sqrt{\frac{2E_i(t)}{T}}\cos(\omega_0 t + \phi)$$

$i = 1, 2, \ldots, M$

$0 \le t \le T$





The general analytic expression for ASK is,

$$s_i(t) = \sqrt{\frac{2E_i(t)}{T}}\cos(\omega_0 t + \phi) \quad \begin{matrix} 0 \le t \le T \\ i = 1, 2, \ldots M \end{matrix} \Bigg\} (1)$$

where the amplitude term $\sqrt{2E_i(t)/T}$ will have M discrete values, and the phase term ϕ is an arbitrary constant.

- M = 2 is chosen because the corresponding waveform is of two types.
- The waveform describes the radar transmission eg. where the two signal amplitude states would be $\sqrt{2E/T}$ and zero.
- The vector corresponding to the maxm amplitude state, and a point at the origin corresponding to the zero amplitude state.
- At the begining of this century, ASK modulation was used in radio telegraphy.

(5) PSK

Analytic waveform

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos(\omega_0 t + 2\pi i M)$$

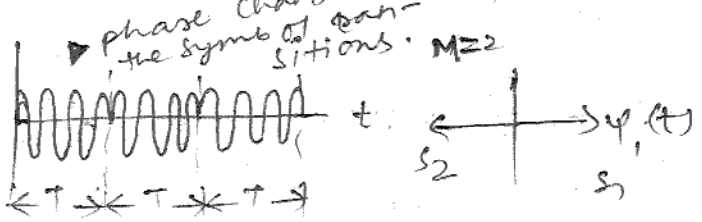
$i = 1, 2, \cdots M$

$0 \le t \le T$

where, the phase term, $\phi_i(t)$, will have M discrete values.

E → symbol energy.
T → symbol time duration.

- It was developed during the early days of the deep-space program.
- In BPSK modulation, the modulating data signal shifts the phase of the waveform $s_i(t)$ to one of two states, either zero or π (180°).
- If the modulating date stream were to consist of alternating ones & zeroes, there would be such an abrupt change at each transition.



- The signal waveforms can be represented as vectors or phasors on a polar plot; the vector length corresponds to the signal amplitude.
- For the BPSK example, the vector picture illustrates the two 180° opposing vectors.
- Signal sets that can be depicted with such opposing vectors are called antipodal signal sets.

c) FSK

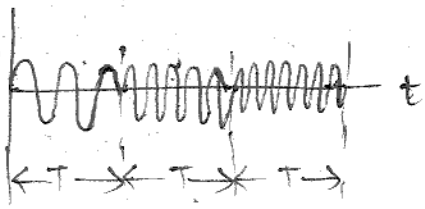
Analytic

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos(\omega_i t + \phi)$$

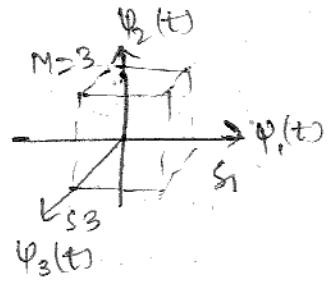
$i = 1, 2, \ldots M$

$0 \le t \le T$

waveform



vector



where, the frequency term ω_i has M discrete values, and the phase term ϕ is an arbitrary constant.

- The waveform of FSK illustrates the typical frequency changes at the symbol transitions.

- At the symbol transitions, the f.s. depicts a gentle shift from one frequency to another.

- In this example, M has been chosen equal to 3, corresponding to the same no. of waveform types; note that this M = 3 choice for FSK has been selected to emphasize the mutually perpendicular axes.

- For an FSK signal set, in the process of meeting the criterion, a condition arises on the spacing b/w the tones in the set.

2] ≃(1) Frequency & phase Synchronization

- Synchronization is a time keeping which requires the co-ordination of events to operate a system in unison.
- ~~phase~~ phase synchronization is the process by which two or more cyclic signals tend to oscillate with a repeating sequence of relative phase angles.
- It is usually applied to two waveforms of the same frequency with identical phase angles with each cycle

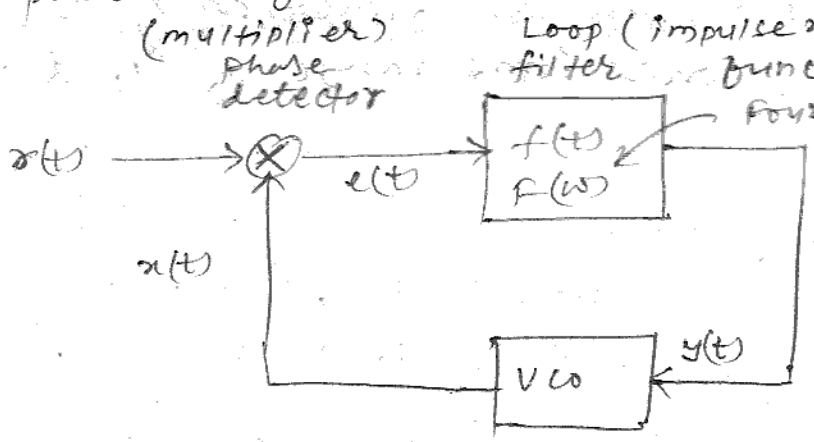


Fig. schematic of the basic phase-locked loop.

- PLLs are servo control loops, whose controlled parameter is the phase of a locally generated replica of the incoming carrier signal.
- It has three components namely a phase detector, a loop filter, and a VCO.
- Phase detector → the device that produces a measure of the diffn in phase b/w an incoming signal & the local replica.

- Incoming signal and the local replica change w.r.t. eachother, the phase diff^{n} (phase error) becomes a time varying signal into the loop filter.

- Loop filter → governs the PLL's response to these variations in the error signal.

- VCO → the device that produces the carrier replica.
  It is a sinusoidal oscillator whose freq. is controlled by a voltage level at the device i/p.

- ~~VCO~~ It is an oscillator whose o/p freq. is a linear function of its i/p voltage over some range of i/p & o/p.

- +ve i/p voltage will cause the VCO o/p freq. to be greater than its uncontrolled value, ω_0, while -ve voltage will cause it to be less.

- phase lock is achieved by feeding a filtered version of the phase difference b/w the incoming signal $x(t)$ & the o/p of VCO, $y(t)$, back to the i/p of VCO, $y(t)$.

Consider a normalized i/p signal of the form,

$$x(t) = \cos[\omega_0 t + \theta(t)] \quad -(1)$$

where, ω_0 → normalized carrier freq.
$\theta(t)$ → slowly varying phase.

$2\sin A \cdot \cos B$
$2\sin A \cdot \sin B$
$2\cos A \cos B$

Similarly, consider a normalized VCO o/p of the form,

$$x(t) = -2\sin[\omega_0 t + \theta_1(t)] \quad \text{— (2)}$$

These signals will produce an o/p error signal at the phase detector o/p of the form:

$$e(t) = x(t) \cdot r(t)$$
$$= 2\sin[\omega_0 t + \theta_1(t)] \cdot \cos[\omega_0 t + \theta(t)]$$
$$= \sin[2\omega_0 t + \theta(t) + \theta_1(t)] + \sin[\theta_1(t) - \theta(t)]$$
$$\approx \sin[2\omega_0 t + \theta_1(t) + \theta(t)] + \sin[\theta_1(t) - \theta(t)] \quad \text{— (3)}$$

The first term of eqn (3) can be ignored because the loop filter is LPF.

- LPF provides an error signal provides an error signal that is solely a function of the ~~diff~~ difference in phases b/w the i/p and the VCO o/p.
- VCO o/p frequency is time derivative of sine function.

The o/p freq. of VCO is a linear funct of ~~time~~ the i/p voltage.

Therefore, since an i/p voltage of zero produces an o/p frequency of ω_0, the diffn in the o/p freq from ω_0 will be proportional to the value of the i/p voltage $y(t)$, or

$$\Delta\omega(t) = \frac{d}{dt}[\theta_1(t)] = K_0 y(t)$$
$$= f_0(t) * K_0 e(t)$$

$= K_o\, e(t) * f(t)$ (loop filter impulse response)

$\cong K_o\,[\theta(t) - \theta_1(t)] * f(t)$ — (4)

↑ Convolution

where,

$\Delta w(t)$ → freq. difference.

K_o → gain of VCO

$e(t) = \sin[\theta(t) - \theta_1(t)] \cong \theta(t) - \theta_1(t)$

small angle approximation, will be accurate when the o/p phase error is small (the loop is close to phase lock).

3) Symbol synchronization

(must include closed loop early/late gate synchronization)

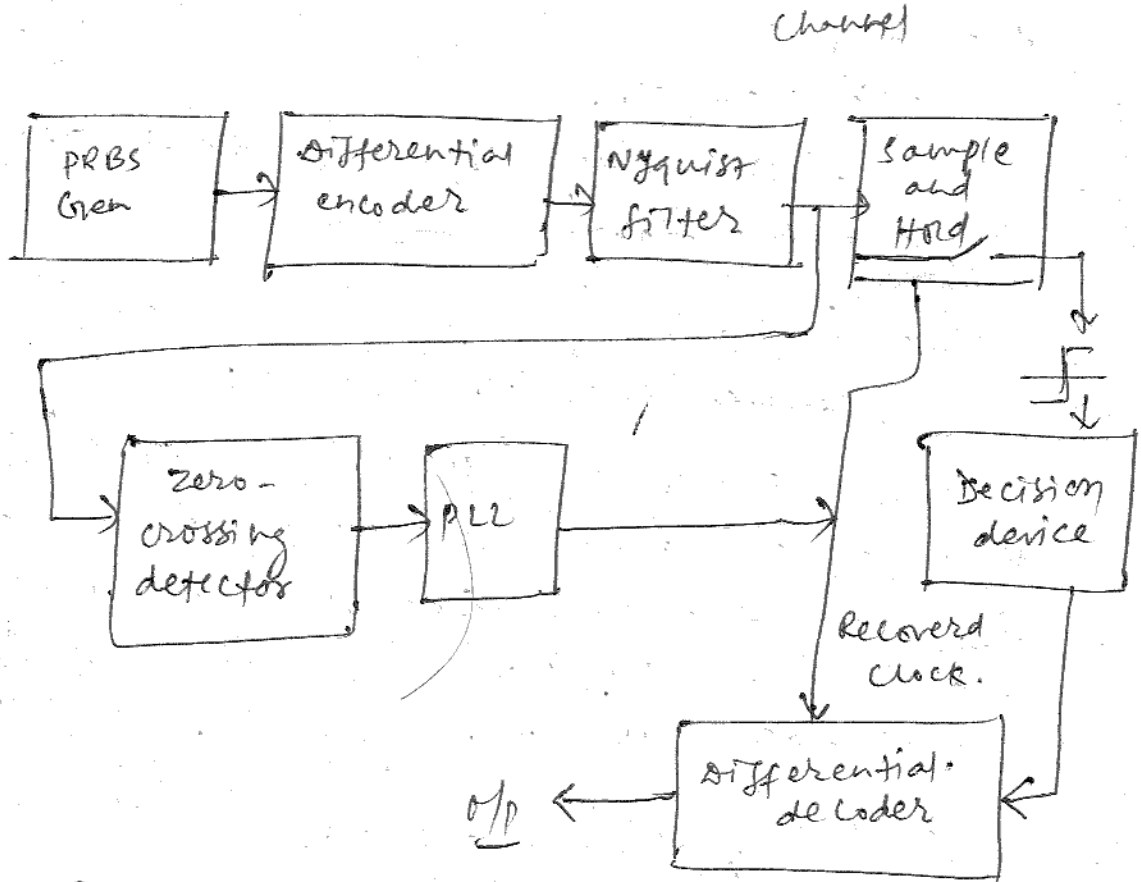


Fig. Completely Baseband communication system with symbol recovery block diagram.

- All digital receivers need to be synchronized to the incoming digital symbol transitions in order to achieve optimum demodulation. For the convenience, we have assumed binary baseband signal.

- It is divided into two groups'.

i) open loop synchronization:

These circuits recover a replica of the transmitter data clock o/p directly from operations on the incoming data stream.

ii) closed loop synchronization:

- to lock a local data clock to the incoming signal by use of comparative measurements on the local and incoming signals.
- It is more accurate, but they are much more costly & complex.

→ It generates freq. component at the symbol rate by operating on the incoming baseband sequence with a combination of filtering and a non-linear device. The operation is analogous to carrier recovery in a suppressed carrier tracking loop.

- For a square-wave i/p, the differential will produce +ve or -ve spikes at all symbol transitions. When rectified, the resulting sequence of +ve

spikes will have a fourier component at the data symbol rate.

- The ipf, however, remove the high frequency components of the data symbols, causing them to lose their original rectangular wave shape. This will cause the resulting differential signal to have some finite rise and and fall time, rather than being a set of impulses.

Closed loop.

- Closed-loop, symbol-data synchronizers use comparative measurements on the incoming signal & locally generated signal. to bring data clock the locally generated signal into synchronism with the incoming data transitions. ~~The procedure is the same as that used for~~

- The most popular closed loop synchronizer is early/late-gate synchronizer.

4] Synchronization with Continuous phase modulation

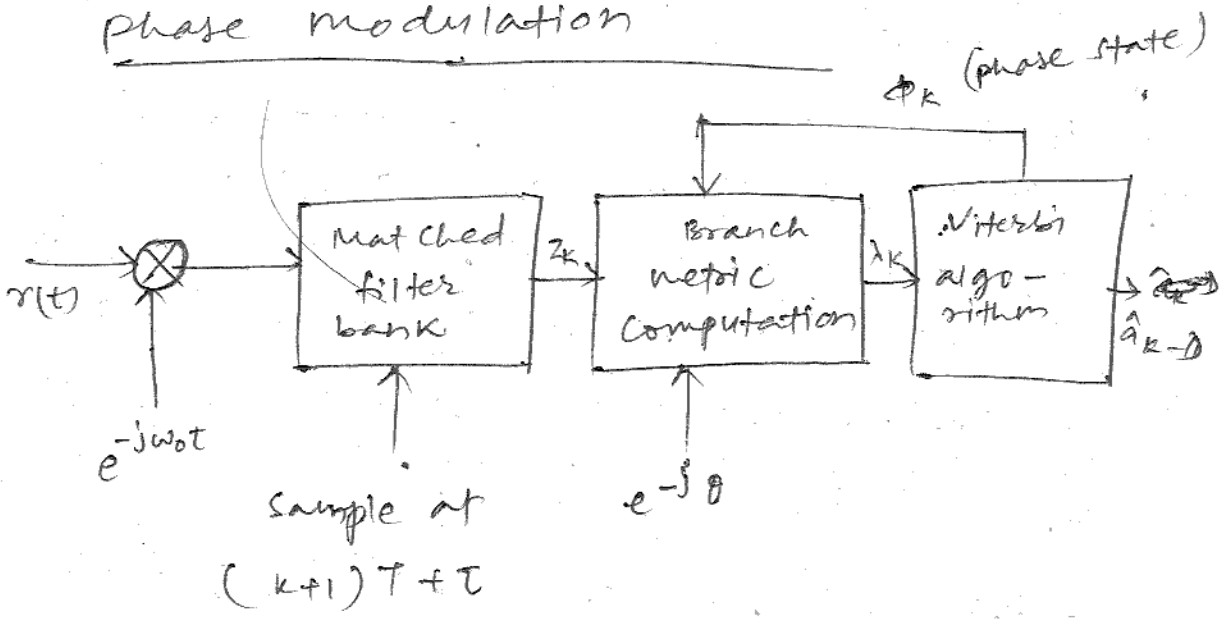


fig CPM receiver

$\hat{a}_{k-D}$ is the k-th. o/p symbol with processing delay, D.

- This modulation raise new issues in synchronization, where the bandwidth efficiency is obtained by increasing the smoothness of the waveforms in the time domain.
- It is difficult with CPM to separate the effects of carrier-phase error from the symbol-timing error, making the phase and timing tasks interrelated.
- In order to reduce or eliminate the high frequency components, one must smooth out all the rough edges or abrupt changes in the time domain signal.

- In CPM signaling, this is accomplished through a combination of three techniques:

i] Use signal pulses that have several orders of continuous derivatives.

ii] Allow individual signal pulses to occupy multiple signal time intervals.

iii] Reduce the max^m allowed phase change per symbol interval.

- For CPM, at the begining of each symbol interval, the excess phase depends only on the phase at the begining of the symbol and the current symbol value.

- The phase value at the begining of the symbol is a consequence of some number of previous symbols. Therefore, if there are finite no. of possible phase states, the result is finite state channel.

- starting the phase transition for the next symbol from this phase state is a necessary condition for continuous phase.

- In the primary signal detection process,

ω_0 → carrier freq.
θ → carrier phase
τ → symbol timing offset

} known

- The receiver structure is effectively a bank of matched filters, each filter matched to an L-symbol signal realization, which feeds a Viterbi Algorithm.

- The set of O/Ps, along with the carrier phase estimate θ, and the phase state Φ_k are used to compute the path metrics, and ~~motion~~ to determine the Viterbi Algorithm's decisions.

5) Frame synchronization

- Almost all digital data streams have some sort of frame structure i.e. the data stream is organized into uniformly sized groups of bits.

- Computer data are typically organized into words of some no. of 8-bit bytes, and these, in turn, are organised into card images, packets, frames, or files.

- For a receiver to make sense of the incoming data stream, the receiver needs to be synchronized with the data stream's frame structure.

- Frame synchronization is usually accomplished with the aid of some special signaling procedure from the Tx.

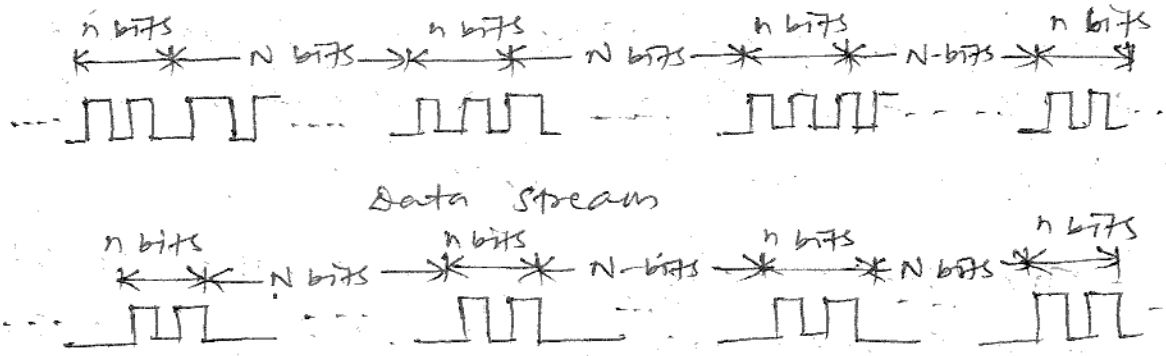


Fig. Frame Marker illustration

- From the above fig. the frame marker is a single bit, or a short pattern of bits that the transmitter injects periodically into the data stream. The receiver must know the pattern and the injection interval.

- The receiver, having achieved data synchronization, correlates the known pattern with the incoming data stream at the known injection interval.

- If the receiver is not in synchronization with the framing pattern, the accumulated correlation will be low;

- when the receiver comes into frame synchronization, the correlation should be nearly perfect.

Advantage:

- It has simplicity.
- Even a single bit can service as a frame marker if a sufficient no. of

correlations are accumulated before deciding wheather or not the system has achieved synchronization.

Advantages:

- The sufficient no. may be very large, and thus, the expected time req^{d} to acquire synchronization would be long.
- The inserted bit(s) may make the organization of the data stream awkward.

Applications:

- used in Television.

6] Network synchronization.

-

- NW synch. deals with the distribution of time and frequency over a network of clocks, including clocks spread over a wide area. The goal is to align the time and frequency scales of all the clocks, by using the communications capacity of links b/w nodes.

- The basic elements of a synchronization n/w are nodes (autonomous & slave clocks) and communication links inter-connecting them.

- In '70's and '80's, most telecommunication operators have set up synchronization n/w's to synchronize their switching and transmission equipment.

- Since the introduction of early digital switching systems, n/w synch. was needed to avoid ~~this~~ slips in ckt. switched voice and data n/w's.

- Traditionally, synchronization has been distributed to telecommunications n/w nodes using ckt-switched links in TDM.

- The terminal txr. parameters are modified to achieve synchronization, rather than modifying the central node's receiver parameters.

- The terminal txr must be synchronized with the system in order for its transmitted burst of data to arrive at the central node at the time when the node is prepared to receive the data.
- Synchronization of the terminal txr. also makes sense with systems that combine signal processing at the central node with FDMA.

- If the terminals precorrect their transmissions to be synchronised with the central node, the node can use a fixed set of channel filters and a single timing reference for the processing of all channels. Otherwise, the node would require a separate time & frequency acquisition and tracking capability for each incoming channel, and it would need to deal with the possibility of varying amounts of adjacent channel interference.

1](a) Direct sequence Spread Spectrum (DS/SS) Txr & Rxr System

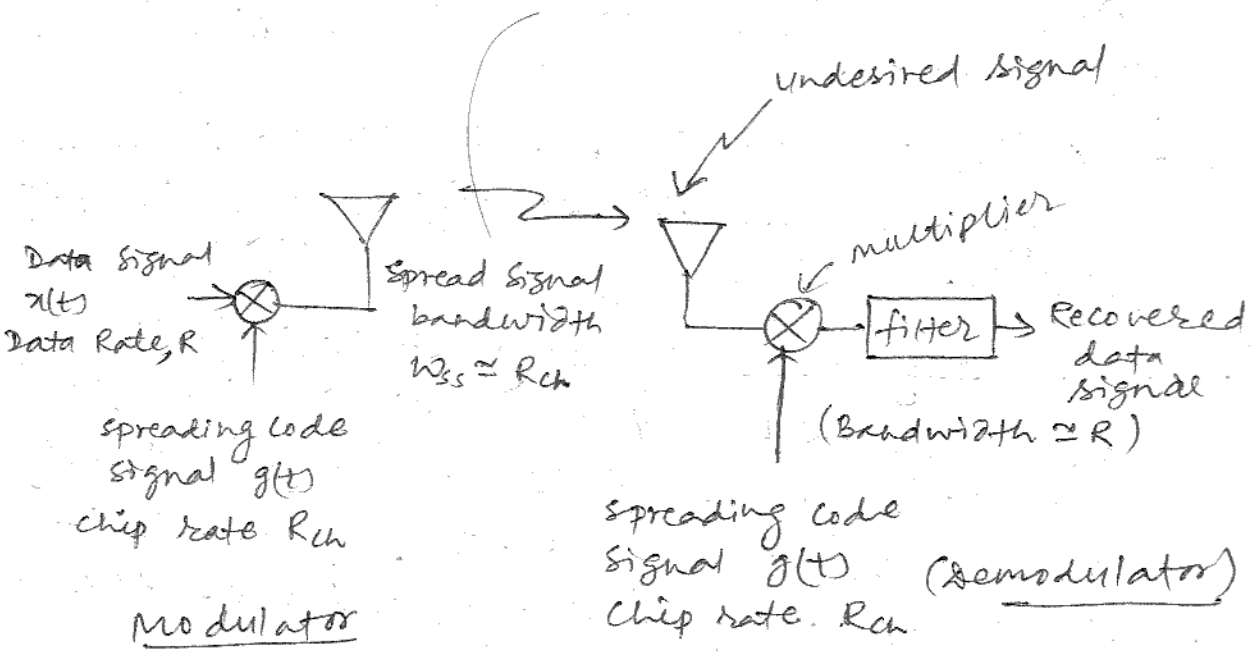


Fig. Basic spread-spectrum technique.

- The above fig. illustrates a model for (DS/SS) interference rejection.
- At the modulator, the information signal x(t), with a data rate of R bits/s, is multiplied by a spreading code signal g(t), having a code symbol rate, called usually called as chip rate, R_{ch} chips/sec.
- Assume, the transmission B.W$_s$ for x(t) and g(t) are R hertz & R_{ch} Hz respectively.
- Multiplication in the time domain transforms to convolution in the frequency domain.

$$x(t) \cdot g(t) \longleftrightarrow X(w) * G(w) \quad -(1)$$

∴ If the data signal is narrowband compared to the spreading signal, the resulting product signal x(t) g(t) will have approximately the B.W. of the spreading signal.

- At the demodulator, the received signal is ideally multiplied by a synchronized replica of the spreading code signal, $g(t)$, which results in the despreading of the signal.

- A filter with B.W. 'R', is used to remove any spurious higher frequency components.

- If any there is any undesired signal at the receiver, the multiplication by $g(t)$ will spread this undesired signal in the same way that the multiplication by $g(t)$ at the txr. spread the desired signal originally.

- Consider the effect on a jammer that attempts to position a narrowband jamming signal within the information B.W.

- The first operation at the rxr. i/p is multiplication by the spreading signal.

- The most important idea behind the interference rejection capability of a spread-spectrum system can be summarized as follow:

i] Multiplication by the spreading signal once spreads the signal B.W.

ii] Multiplication by the spreading signal twice, followed by filtering, recovers the original signal.

iii] The desired signal gets multiplied twice, but the interference signal gets multiplied only once.

b) Merits :

- privacy, secure communications because signal is 'hidden' like noise.
- Non-interference with other signals in the same band.
- possible to share frequency and time at the same time (CDMA).
- protection against jamming.
- fine time resolution.

Demerits.

- Increase bandwidth.
- Increase complexity.

2. a] Frequency hop spread spectrum tsr. and rxr.

- FHSS systems operate with narrow band signals located around different carrier frequencies.
- If at a specific moment, the FHSS system is using a carrier frequency significantly faded as a result of multipath, the FHSS receiver could not get enough energy to detect the radio signal.
- The resultant loss of information is corrected by re-transmitting the lost packets.

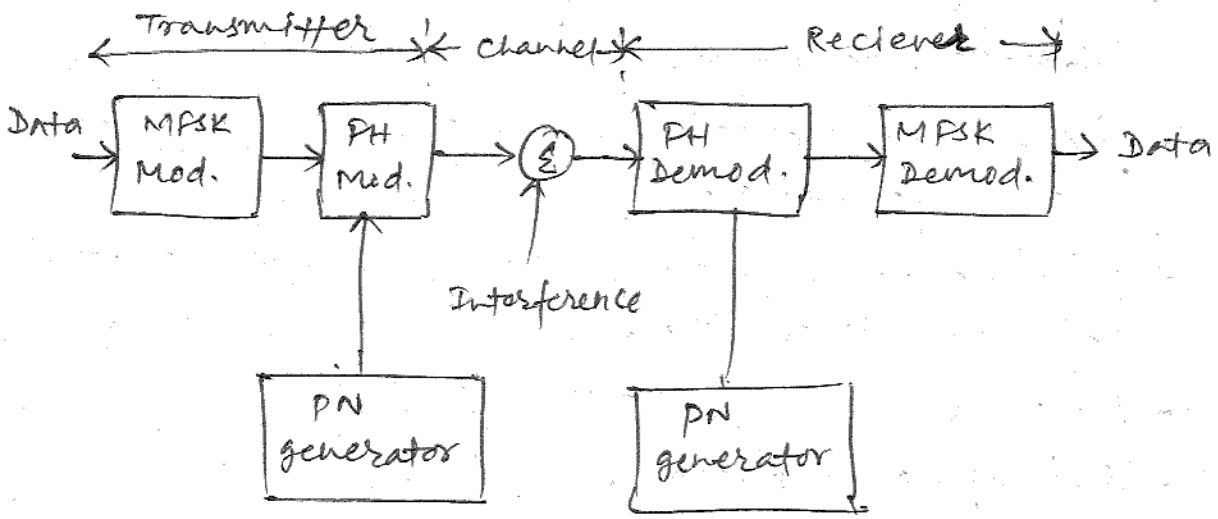


Fig. FHSS system.

- consider FHSS technique where M-ary freq. shift keying technique is used, where $k = \log_2 M$ information bits are used to determine which one of M freq. is to be determined.

- The FH system operates two-step modulation process - data modulation and freq. hopping modulation - even though it can be implemented as a single step.

- At each frequency hop time, a PN generator feeds the freq. synthesizer a frequency word.

- The frequency-hopping bandwidth W_{ss}, and the minm freq. spacing b/w consecutive hop positions Δf.

- For a given hop, the occupied transmission B.W is much smaller than Wss.
- Spread-spectrum technology permits FH B.Ws of the order of several GHz, which is an order of magnitude larger than implementable DS bandwidths.
- Since frequency hopping techniques operate over such wide bandwidths, it is difficult to maintain phase coherence from hop to hop.
- Therefore, such schemes are usually configured using non coherent demodulation.

- The receiver reverses the signal procesing steps of the txr.
- The received signal is first FH demodulated (dehoped) by mixing it with the same sequence of pseudorandomly selected freq. tones that was used for hopping.
- Then the dehoped signal is applied to a conventional bank of M non-coherent energy detectors to select the most likely symbol.

b) Soln:

Given: $T_b = 4.095ms$, PN chip duration, $T_c = 1\mu s$

$\frac{E_b}{N_0} = 10$, for average probability of error less than 10^{-5}

sometimes, the one bit period of PN sequence is also called as one 'chip'.

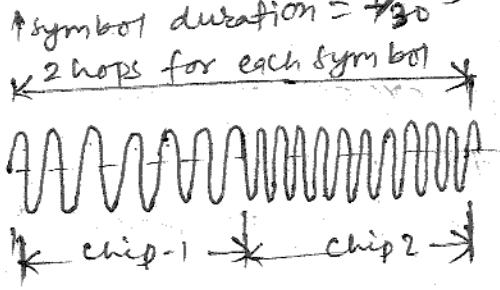
processing gain:

$$PG = \frac{T_b}{T_c} = \frac{4.095 \times 10^{-3}}{1 \times 10^{-6}} = \boxed{4095} \quad [\because PG = N = 4095]$$

Jamming margin: $= \frac{J}{P_s} = \frac{PG}{E_b/N_0} = \frac{4095}{10} = \boxed{409.5}$

3(a) Frequency
Fast hopping : hops/bit

- one data bit is divided over multiple hops.
- In fast hopping, coherent signal detection is difficult and seldom used.
- Mostly ASK, FSK, PSK modulation is used.
- There are several freq. hops per modulation symbol.
- For FFH, the shortest interrupted waveform is that of the hop.

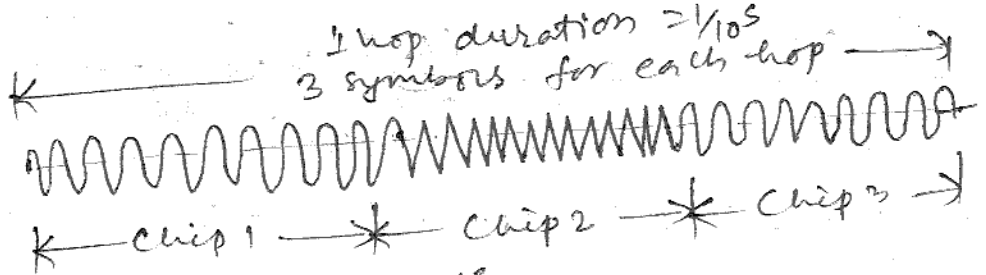


= ½ symbol duration
= 1/60 s

- The above fig. illustrates an example of FFH, the data symbol rate is 30 symbols/s & the frequency hopping rate is 60 hops/s.
- The fig. illustrates the waveform s(t) over one symbol duration in ~~60 hops/s~~ is (1/30 s)
- The waveform change in s(t) is due to a new frequency hop.
- In this example, a chip corresponds to a hop since the hop duration is shorter than the symbol duration.
- ~~hop < bits~~ each chip corresponds to half symbol.

Slow frequency Hoping (SFH): bits/hopes)

- In this case one or more data bits are transmitted within one hop.
- Coherent data detection is possible.
- Often, systems using slow hopping also employ (burst) error control coding to restore loss of (multiple) bits in one hop.
- It avoids that a stationary terminal that happens to be located in a fade looses its link to the base station.
- SFH systems change frequency at a rate comparable with (slower than) the information rate.



= 1 symbol duration
= 1/30 s

- Above fig. illustrates an example of SFH, the data symbol rate is still 30 symbols/s, but the frequency hoping rate has been reduced to 10 hops/s.
- The waveform s(t) is shown over a duration of three symbols ($\frac{1}{10}$ s).

- Here, the changes in the waveform are due to the modulation state changes;
- Therefore, a chip corresponds to a data symbol.
- Data symbol is shorter than the hop duration.

b) Method of Generation of ~~pseudo~~ Pseudonoise sequence.

A pseudo noise (PN) sequence is a sequence of binary numbers.

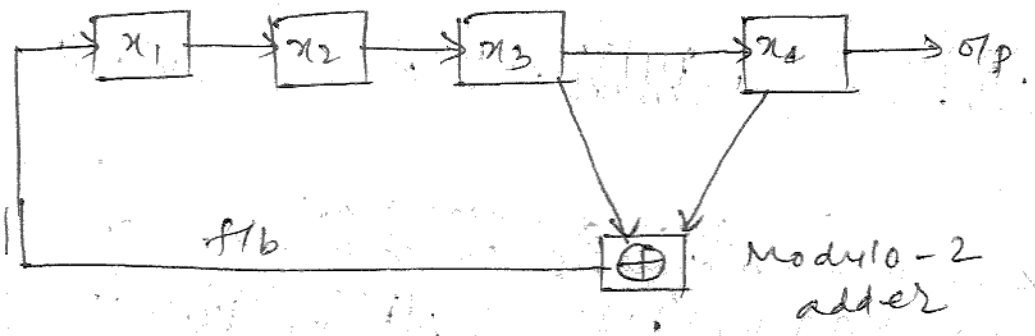


fig. Linear f/b shift register.

- Consider a linear f/b shift register which is made up of 4-stage register for storage and shifting, a modulo-2 adder, and a f/b path from the adder to the i/p of the register.

- The shift register operation is controlled by a sequence of clock pulses.
- At each clock pulse, the contents of stages x_3 and x_4 are modulo-2 added, & the result is fed back to stage x_1. The shift register sequence is defined to be the o/p of the last stage - stage x_4.
- The o/p sequence is obtained by noting the contents of stage x_4 at each clock pulse.

- The shift register generator produces sequences that depend on the no. of stages, the f/b tap connections, & initial conditions.

- The o/p sequences can be classified as either maximal length or non-maximal length.

4(a) properties of maximum length sequence.

⇒ The fig. is similar to 3(b). Apart from those,

- Assume that stage x_1 is initially filled with a one and the remaining stages are filled with zeroes. i.e. the initial state of the register is 1000.

From fig. The succession of register states will be as follows:

1000 0100 0010 1001 1100 0110 1011 0101
1010 1101 1110 1111 0111 0011 0001 1000

since, the last state, 1000, corresponds to the initial state, we see that the register repeats the forgoing sequence after 15 clock pulses.

- The o/p sequence is seen to be

0 0 0 1 0 0 1 1 0 1 0 1 1 1 1

where, the left most bit is the earliest bit.

- The shift generator produces sequences that depend on the no. of stages, the f/b tap connections, and initial conditions.
- maximal length sequences have the property that for an n-stage linear feedback shift register, the sequence repetition period in clock pulses P is

$$P = 2^n - 1 \quad \text{— (1)}$$

- Thus, from ①, it can be seen that the sequence generated by the shift register generator of above fig. is an eg. of maximal length sequence.

- If the sequence length is less than $(2^n - 1)$, the sequence is classified as a non-maximal length sequence.

b] Spread spectrum communication system.

- In spread spectrum technique, the transmission B.W. employed is much greater than the minm B.W. reqd to transmit the information.

- It can be said spread-spectrum system if it fulfills the following requirements:

i) The signal occupies a B.W. much in excess of the minm B.W necessary to send the information.

ii) Spreading is accomplished by means of a spreading signal, often called a code signal, which is independent of the data.

iii) At the receiver, despreading is accomplished by the correlation of the received spread signal with a synchronized replica of the spreading signal used to spread the information.

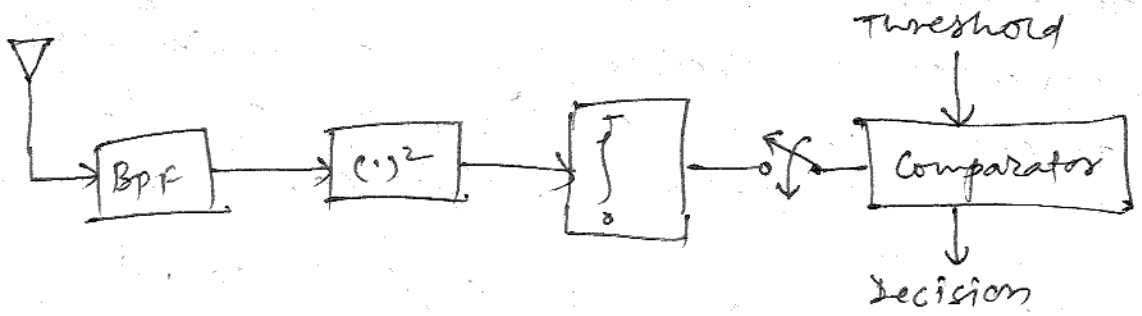


fig. Radiometer

- A radiometer is a simple power measuring instrument that can be used by an adversary to detect the presence of spread spectrum signals within some bandwidth W.

- The above fig. consists of BPF. with B.W W, a squaring circuit to ensure a +ve o/p value, and an integrating ckt.

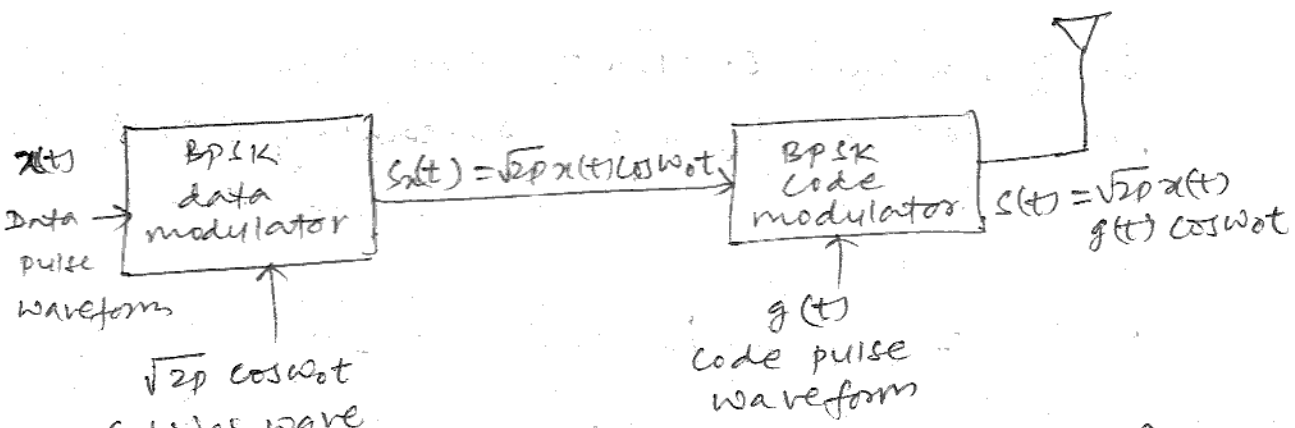
- At time t=T, the o/p of ~~Comparator~~ integrator is compared to a present threshold.

→ If o/p of the integrator > threshold, a signal is declared present, otherwise the signal is declared absent.

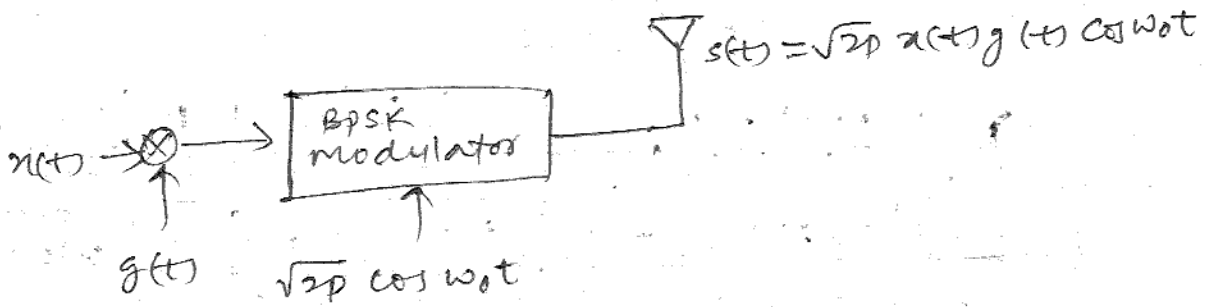
→ SS systems that are designed to exhibit LPI may also exhibit a low probability of position fix (LPPF), which means that even if the presence of the signal is perceived, the dirn of the tar. is difficult to pinpoint.

- By spreading the downlink energy over a wider B.W, the total transmitted power can be increased and hence performance improved,
- spread spectrum signals can be used for
- ranging or determination of position location.

5) a) Performance of DSSS system



(a) DS modulator (~~Rx~~ Tx.)



(b) Simplified BPSK DSS Tx.

- The block diagram depicts a direct-sequence (DS) modulator.

- A carrier wave is first modulated with a data signal $x(t)$, then the data-modulated signal is again modulated with a high speed (wide-band) spreading signal $g(t)$.

- The constant-envelope data-modulated carrier is, given by,

$$s_x(t) = \sqrt{2P} \cos [\omega_0 t + \theta_x(t)] \quad -①$$

where,

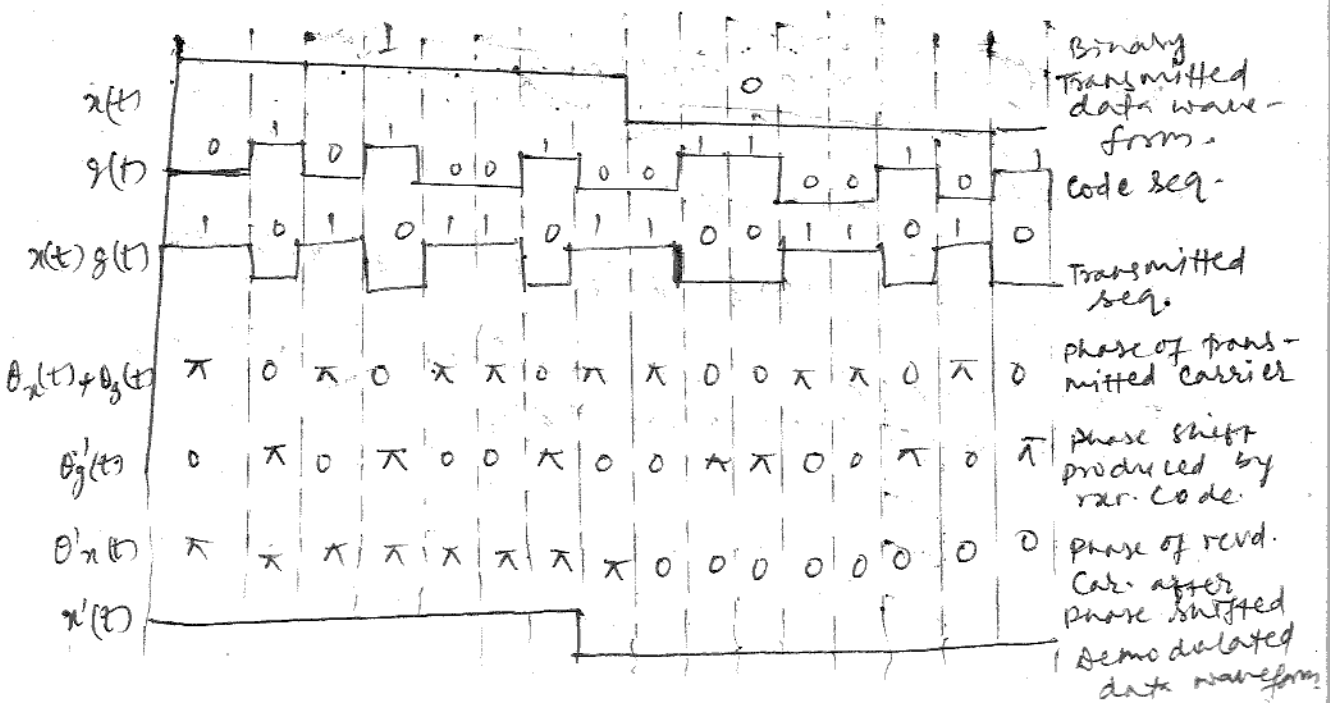
$P \rightarrow$ power,
$\omega_0 \rightarrow$ radian freq.
$\theta_x(t) \rightarrow$ data phase modulation.

Using further constant-envelope modulation by the spreading signal, $g(t)$; the transmitted waveform can be expressed as,

$$s(t) = \sqrt{2P} \cos [\omega_0(t) + \theta_x(t) + \theta_g(t)] \quad -②$$

$\theta_x(t) \rightarrow$ phase of the carrier due to data

$\theta_g(t) \rightarrow$ phase of carrier due to spreading sequence.



(5) Soln:

i) ~~Given~~, To obtain the PN sequence

There are Four stages of s/b shift registers.

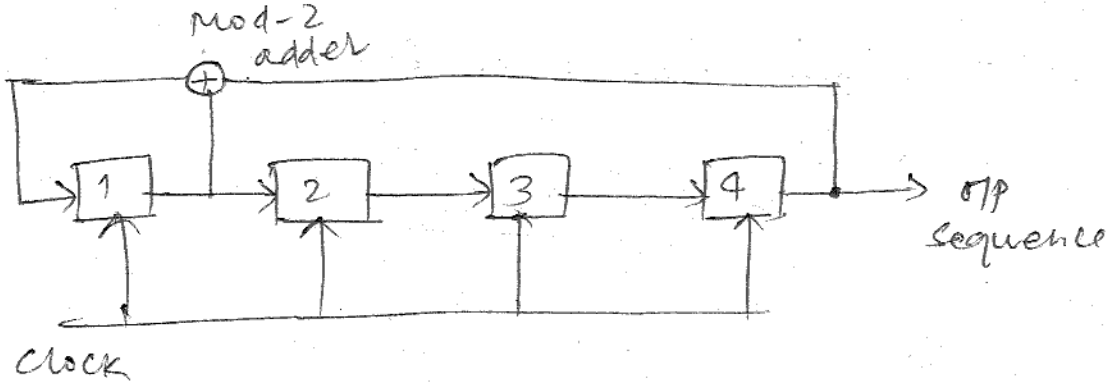


Fig. A four-stage shift register to generate PN sequence.

The generated PN sequences are:

shift no.	state of shift register				Mod-2 adder O/P	PN-sequence
					$S_3 \oplus S_4$	S_4
0	1	0	0	0	1	0
1	1	1	0	0	1	0
2.	1	1	1	0	1	0
3.	1	1	1	1	0	1
4	0	1	1	1	1	1
5.	1	0	1	1	0	1
6.	0	1	0	1	1	1
7	1	0	1	0	1	0
8.	1	1	0	1	0	1
9.	0	1	1	0	0	0
10	0	0	1	1	1	1
11	1	0	0	1	0	1
12	0	1	0	0	0	0
13	0	0	1	0	0	0
14	0	0	0	1	1	1
15	1	0	0	0	1	0

(14)

ii) To obtain chip duration.

$$T_c = \frac{1}{R_c} = \frac{1}{10^7} \text{ sec} = \boxed{0.1 \text{ MS}}$$

iii) To obtain length of PN sequence:

$$N = 2^m - 1$$
$$= 2^4 - 1 = \boxed{15 \text{ digits.}}$$

iv) To period of o/p sequence is,

$$T_b = NT_c$$
$$= 15 \times 0.1 \text{ MS}$$
$$= \boxed{1.5 \text{ MS}}$$

UNIT-V

3]. AES algorithm: (computer security standard).

← operates on a 4×4 major order.

- Advanced Encryption standard (AES) is a specification for the encryption of electronic data.
- It is based on a design principle known as a substitution permutation network.
- It is fast in both software & hardware.
- AES has fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
- There are four stages for the AES algorithm as below:
  i] sub bytes
  ii] shift rows
  iii] mix columns
  iv] Add round key.

Step-I : sub Bytes

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

sub-Bytes →

b_{00}	b_{01}	b_{02}	b_{03}
b_{10}	b_{11}	b_{12}	b_{13}
b_{20}	b_{21}	b_{22}	b_{23}
b_{30}	b_{31}	b_{32}	b_{33}

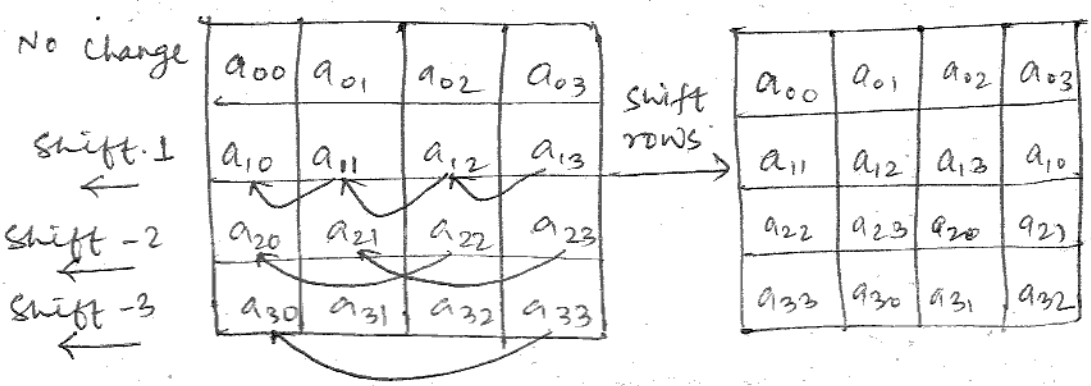
a_{22} → [S] → b_{22}
(S: substitution box)

- In this step, each byte in the state is replaced with its entry in a fixed 8-bit.

S: $b_{ij} = S(a_{ij})$

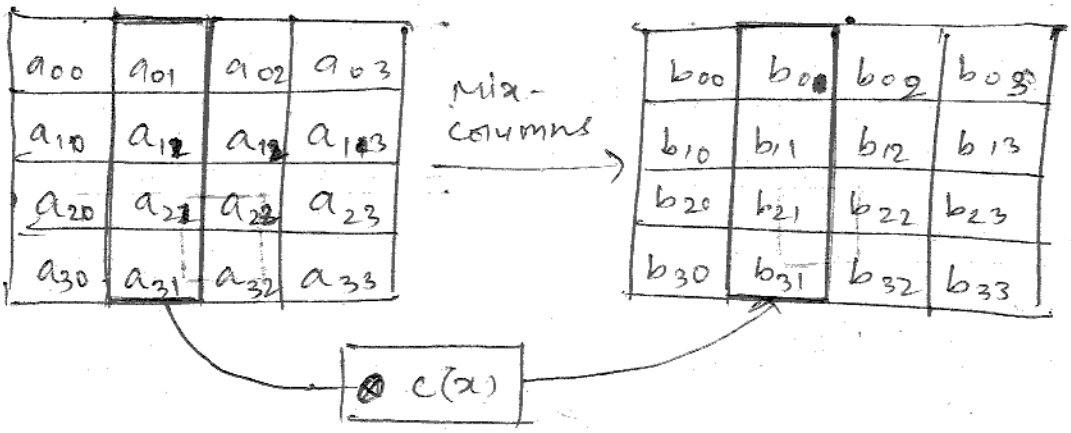
- Each byte in the matrix is updated using an 8-bit substitution box (S), & the Rijndael S-box.
- This operation provides the non-linearity in the cipher.
- S-box is also chosen to avoid any fixed points, and also any opposite fixed points.

Step-II : Shift Rows.



- In this step, the bytes in each of the State are shifted cyclically to the left. The no. of places each byte is shifted differs for each row.
- In this way, each column of the o/p state of the shift rows step is composed of bytes from each column of the input state.

Step-3 : The Mix Columns step



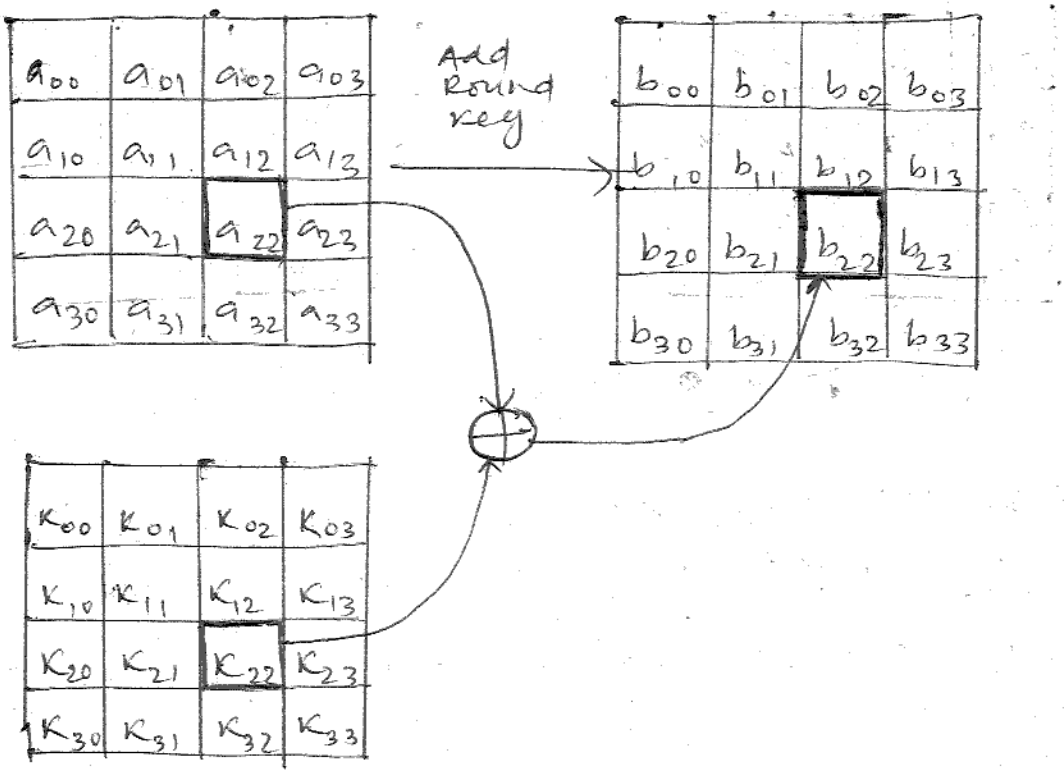
- In this step, each column of the state is multiplied with a fixed polynomial c(x).

where, the known matrix for 128 bit key is,

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

- multiplied by 1 means - leaving uncharged.
- " " 2 " shifting byte to the left.
- " " 3 " shifting to the left and then performing XOR with the initial unshifted value.

Step-4 : Add Round key step



- In this step, each byte of the state is combined with a byte of the round sub key using the XOR operation (⊕).

4) RSA algorithm (Rivest - shamir - Adleman) :

- RSA is an internet encryption and authentication system that uses an algorithm.

- The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the web browers from Microsoft and Netscape.

Algorithm

- There involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and private key.

- once the keys have been developed, the original prime numbers are no longer important and can be discarded.

- Both the public and private keys are need for encryption ~~and~~/ decryption but only the ~~owes of~~ owner of a private key ever needs to know it.

- Using the RSA system, the private key never needs to be sent across the Internet.

- The private key is used to decrypt text that has been encrypted with the public key.

To do this

- Send an encrypted message.
- " " " signature.
- Decrypt an encryted message.
- " " " signature (and authenticate the sender).

5] public key cryptography.

- public key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and other to unlock or decrypt the cyphertext.

- Neither key will do both functions.
- one of these key is published or public and the other is kept private.

- If the lock/encryption key key is the one published then the system enables private communication from the public to the unlocking key's owner.

- If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the ~~owner~~ owner of the private key.
- It is a fundamental and widely used.

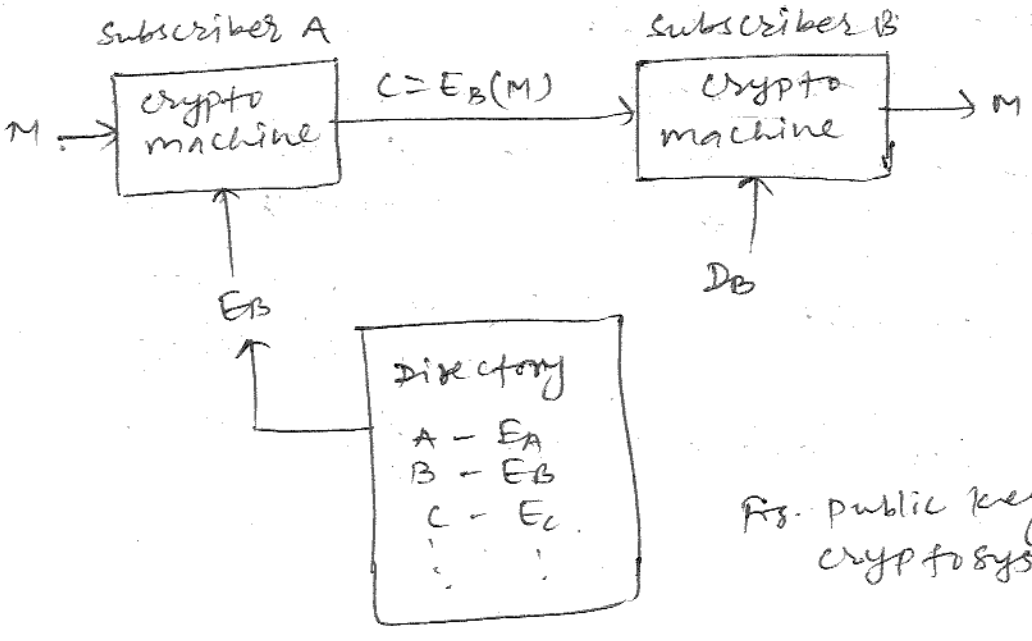


Fig. public key cryptosystem.

The important features of a public key cryptosystems are:

i) The encryption algorithm E_K and the decryption algorithm D_K are invertible transformations on the plaintext M, or the ciphertext C, defined by the key K.

i.e. For each K and M, if $C = E_K(M)$,

then $M = D_K(C) = D_K[E_K(M)]$.

ii] For each K, E_K and D_K are easy to Compute.

~~iii)~~

Such a system would enable secure communication b/w subscribers who have never communicated before. for eg. in fig.

Subscriber A can send a ~~msg~~ msg, M, to subscriber B by looking up B's encryption key in the directory.

- Encryption algorithm, E_B, he helps to obtain the ~~cipher~~ Ciphertext $C = E_B(M)$, which transmits on public channel.

- subscriber B is only the party who can decrypt C by applying his decryption algorithm, D_B, to obtain $M = D_B(C)$.

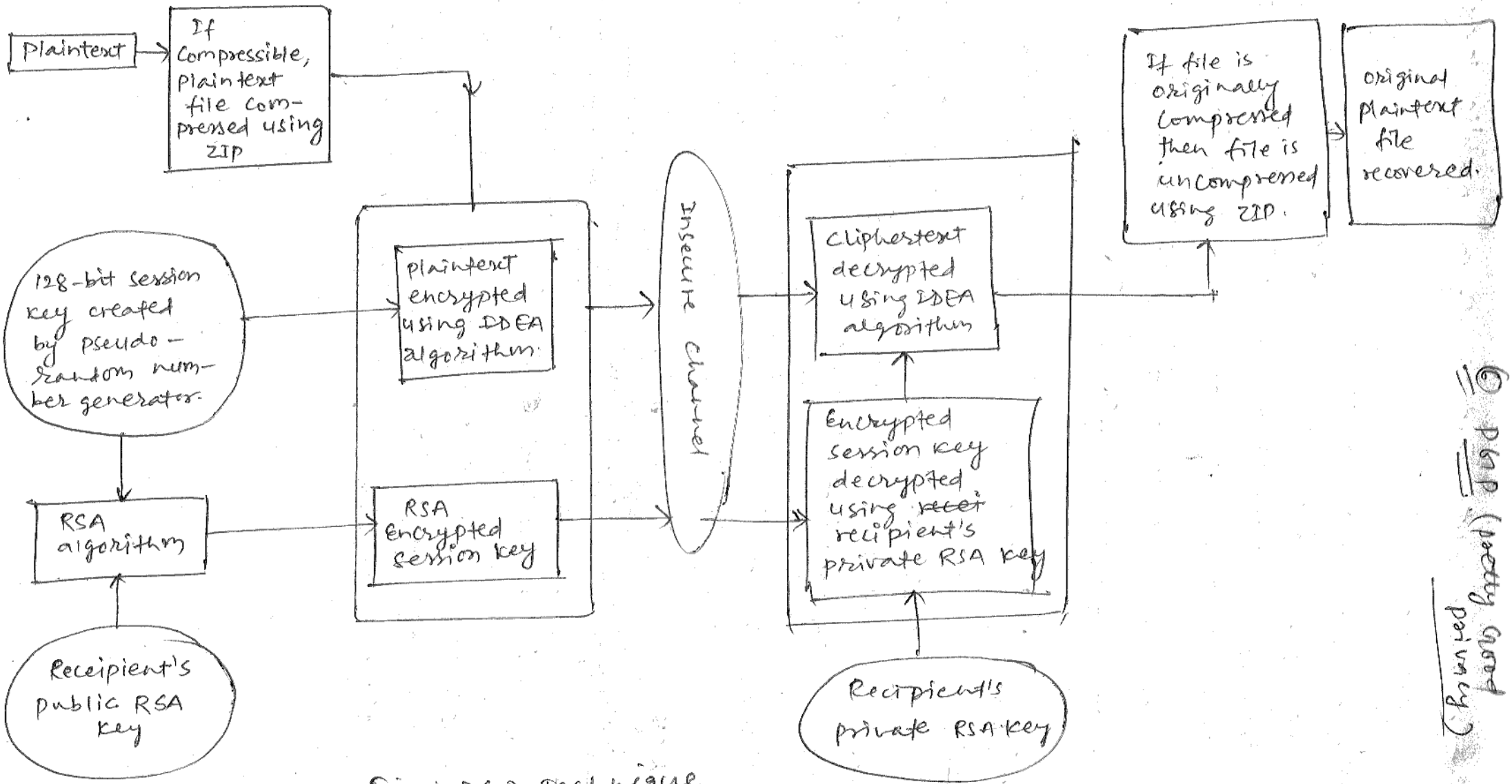


Fig: PGP Technique.

6. PGP (Pretty Good Privacy)

- The technique for message encryption employed by PGP is illustrated where the plaintext is compressed with the ZIP algorithm prior to encryption.
- If the compressed text is shorter than the uncompressed text, the compressed text will be encrypted, otherwise the uncompressed text is encrypted.
- Data compression removes redundant character strings in a file and produces a more uniform distribution of characters.
- Compression provides a shorter file to encrypt and decrypt, but compression is also advantageous because it can hinder some cryptanalytic attacks that exploit redundancy.
- As shown in fig, PGP begins file encryption by creating a 128-bit session key using a pseudo-random number generator.
- The compressed plaintext file is then encrypted with the IDEA private-key algorithm using this random session key.
- The random session key is then encrypted by the RSA public-key algorithm using the recipient's key.

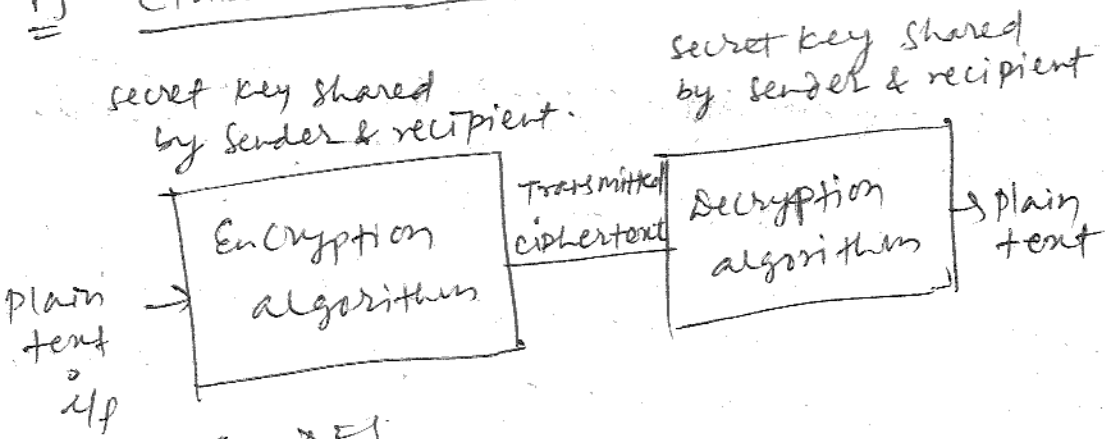
- The RSA encrypted session key and the IDEA-encrypted file are sent to the recipient.

- When the recipient's needs to read the file, the encrypted session key is first decrypted with RSA using the recipient's private key.

- The ciphertext file is then decrypted with IDEA using the decrypted session key.

- After uncompression, the recipient can read the plaintext file.

1] Classical Encryption Techniques:



Eg. DES

Fig. Classical Encryption

- In early time, the letters of plaintext are replaced by other letters or by numbers or symbols.

- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

- one of the earliest examples of a mono alphabetic cipher was the Ceaser cipher, used by Julius caesar during the Gallic wars.

- Each plaintext ~~is~~ ~~as~~ letter is replaced with a new letter obtained by an alphabetic shift.

- The below fig illustrates such an encryption transformation, consisting of three end-around shifts of the alphabet.

- when using this ~~cea~~ Caesar's alphabet, the message, 'Go there' is encrypted as follow:

plaintext : G O T H E R E
ciphertext : J R W K H U H

fig. Caesar's alphabet shift.

- The decryption key is simply the no. of alphabetic shifts; the code is changed by choosing a new key.

- Another classic cipher system, illustrated below fig. is called the Polybius square.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

5x5 array

Polybius square.

- Letters I & J are first combined and treated as a single character.

Plaintext: G O T H E R E

Ciphertext: 22 43 44 32 51 24 51.

- The code is changed by a rearrangement of the letters in the 5x5 array.

2) DES Algorithm : (Data Encryption Standard)

- Data Encryption Standard (DES) is a widely used method of data encryption using a private key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries.

- ~~It was selected by~~

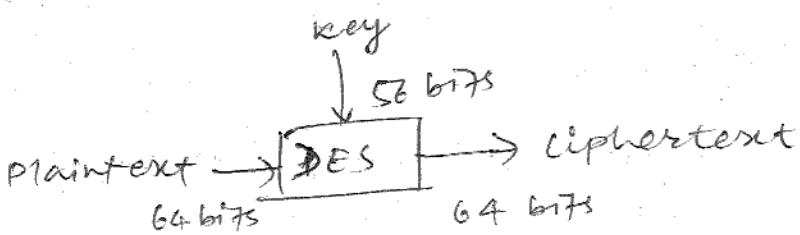


fig. Data Encryption ~~sg~~ Standard viewed as a block encryption system.

- It is based on a symmetric-key algorithm that uses a 56-bit key.
- After a lot many controversies, DES consequently came under intense academic scrunity which motivated the modern understanding of block ciphers and their cryptanalysis.
- An i/p block of 64 bits, regarded as a plaintext symbol in this alphabet, is replaced with a new ciphertext symbol.

- The encryption algorithm starts with an initial permutation (IP) of the 64 plain text ~~bits~~ bits, described in the IP table.

- After this initial permutation, the heart of the encryption algorithm consists of 16 iterations using the standard building block.

- The SBB uses 58 bits of key to transform the 64 i/p data bits into 64 o/p data bits, designed as 32 left-half bits & 32 right-half bits.

- The o/p of each building block becomes the i/p of to the next building block.

- The i/p right half 32 bits (R_{i-1}) are copied unchanged to become the o/p left half 32 bits(L_i).

- The R_{i-1} bits are also extended and transformed into 48 bits with the E-table, and then modulo-2 summed with the 48 bits of the key.

- As in the case of the IP table, the E-table is read from left to right and from top to bottom. The table expands bits

$$R_{i-1} = x_1, x_2, \ldots x_{32}$$

into $(R_{i-1})_E = x_{32}, x_1, x_2, \ldots x_{32}, x_1$ — (1)