Q4:

(a) ASK behaves like baseband OOK for error rate purposes and is particularly susceptible to noise because information is conveyed by amplitude. For a carrier peak amplitude of Ac, coherent transmission with noise power σ

$$P_e = \frac{1}{2} erfc\left(\frac{A_c}{2\sqrt{2}\sigma} \right)$$

FSK and PSK have a carrier present at all times producing

$$P_e = \frac{1}{2} erfc\left(\frac{A_c}{2\sigma} \right) \text{ and } P_e = \frac{1}{2} erfc\left(\frac{A_c}{\sqrt{2}\sigma} \right) \text{ respectively}$$

In both cases, the ratio A_c/σ is divided by a smaller number so the probability of error will be less as the SNR is increased.

FSK spectrum is like 2 ASK signals spaced by the frequency deviation , PSK has same bandwidth as ASK.

ASK bandwidth is $2B_T$ for bit rate B_T
FSK bandwidth is $2B_T + \Delta f$
PSK bandwidth is $2B_T$
So PSK becomes attractive when bandwidth is limited.

(b) For FSK, using f_1 and f_0 the pulses exist 0 to T.

$$\int_0^T p^2(t)dt = \int_0^T A_c{}^2 \cos^2(2\pi f_1 t) + A_c{}^2 \cos^2(2\pi f_0 t) - 2A_c^2 \cos(2\pi f_1 t)\cos(2\pi f_0 t)dt$$
$$= \frac{A_c^2}{2}\int_0^T \{1+\cos(4\pi f_1 t)\}dt + \frac{A_c^2}{2}\int_0^T \{1+\cos(4\pi f_0 t)\}dt - 2A_c^2\int_0^T \cos(2\pi f_1 t)\cos(2\pi f_0 t)dt$$

$\approx A_c^2 T$ provided $|f_1 - f_0| >> B_T$ so that there are many cycles in T

Now the energy per bit is

$$E_b = \frac{1}{2}\int_0^T A_c{}^2 \cos^2(2\pi f_1 t)dt + \frac{1}{2}\int_0^T A_c{}^2 \cos^2(2\pi f_1 t)dt$$
$$E_b = \frac{A_c^2}{4}\int_0^T \{1+\cos(4\pi f_1 t)\}dt + \frac{A_c^2}{4}\int_0^T \{1+\cos(4\pi f_0 t)\}dt$$

Under the same condition of $|f_1 - f_0| >> B_T$

$$E_b = \frac{A_c^2 T}{2}$$

Now,

$$P_e = 0.5\,\mathrm{erfc}\sqrt{\frac{\int_{-\infty}^{\infty} p^2(t)dt}{4N_0}}$$

$$P_e = 0.5\,\mathrm{erfc}\sqrt{\frac{A_c^2 T}{4N_0}} = 0.5\,\mathrm{erfc}\sqrt{\frac{E_b}{2N_0}}$$

(c) Given $A_c = 0.5V$ and $T = 1/100\times10^3 = 10^{-5}\,s$

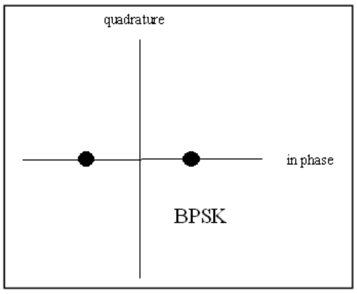
$$E_b = \frac{A_c^2 T}{2} = \frac{0.25}{2}\times10^{-5} = 1.25\times10^{-6}\,J$$

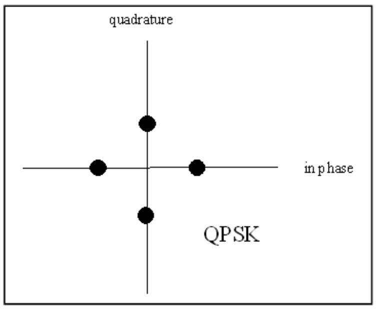
$$\frac{N_0}{2} = 3.8\times10^{-8}\,\mathrm{V^2Hz^{-1}} \Rightarrow N_0 = 7.6\times10^{-8}\,\mathrm{V^2Hz^{-1}}$$

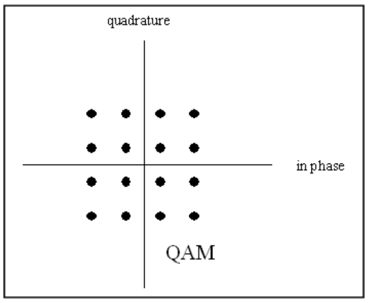
$$P_e = 0.5\,\mathrm{erfc}\sqrt{\frac{1.25\times10^{-6}}{2\times7.6\times10^{-8}}} = 0.5\,\mathrm{erfc}(2.868)$$

$$= \frac{0.5\times\exp\left(-2.868^2\right)}{2.868\sqrt{\pi}} = 2.63\times10^{-5}$$

(d) If we have B Hz of usable bandwidth the data rate may be increased by transmitting more information per symbol using multi-level signalling. For example in ASK if we use 4 amplitude levels instead of 2 then each symbol represents 2 bits of information and the data rate becomes 2B bits/s. Increasing from 2 to M levels increases our data rate to log2M × B bits/s which enables higher data rates without the requirement for more bandwidth.



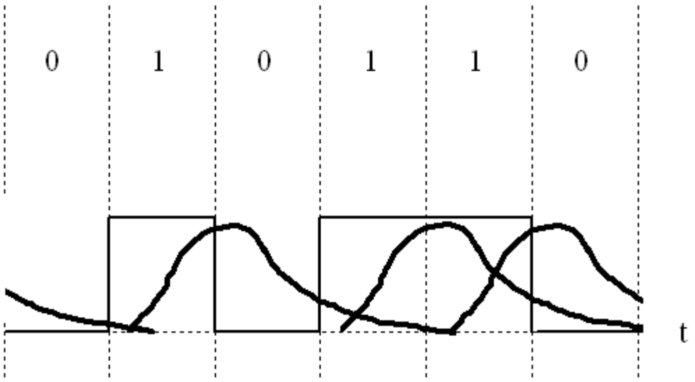




Q5:

(a) In an ideal world we would like a signal to be transmitted through a particular transmission system without distortion. If x(t) is transmitted the output y(t) should be a delayed copy of this, i.e. $y(t) = Kx(t - t_0)$ where the t0 is the transmission delay, and K is a constant (attenuation). However, real channels often behave as low pass filters (LPFs)

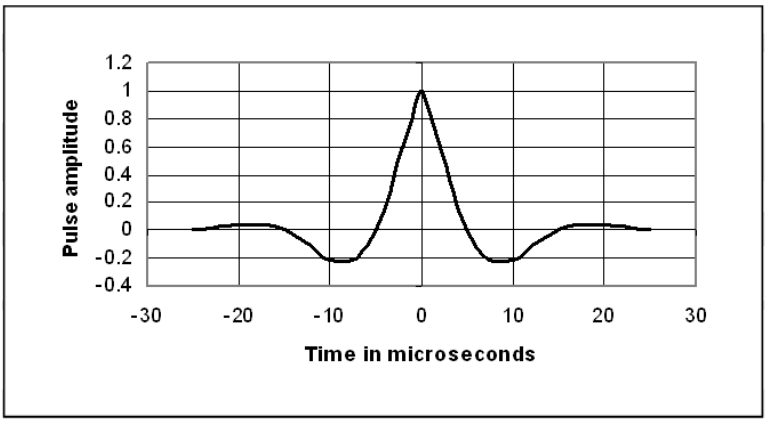
Baseband digital signals normally originate in rectangular pulse form (because they are easy to generate) and consequently have a wide bandwidth (sin(x)/x). This can result in significant distortion when passing through LPF channels but we might accept some distortion which would result from using a bandlimited version of the signal. Bandlimiting leads to the signal element spreading in the time domain (a narrow spectrum in one domain $\Rightarrow$ a wide one in the other) and eventually "overflowing" into the adjacent time slots. This "intersymbol interference" (ISI) can lead to errors as the zeros in particular will disappear as shown below and become very susceptible to noise.



(b) The pulse given is

$$p(t) = e^{-\pi B|t|/2}\cos(\pi B t)$$

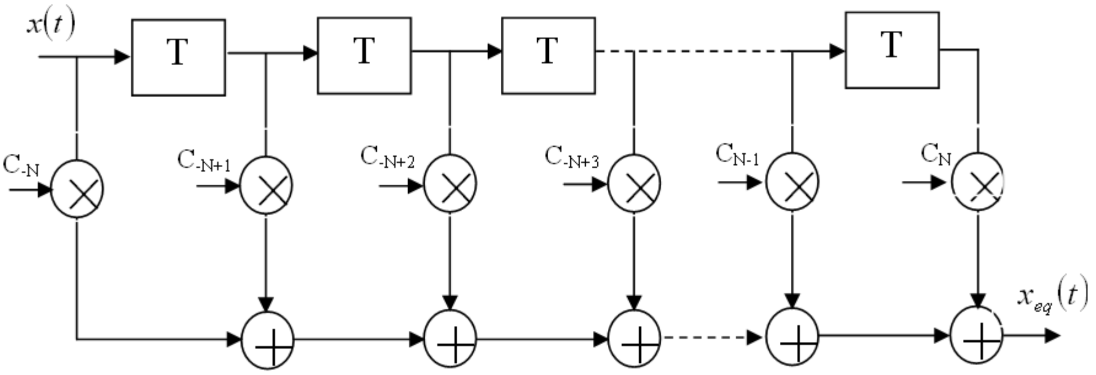
for B = 100 kHz. Calculation of points gives



(c) Irrespective of pulse shape, some residual ISI remains in the output as a result of imperfect filter design and incomplete knowledge of the channel. An equaliser is used between the receiving filter and the decision device. A popular configuration for an equaliser is a finite impulse response (FIR) filter structure.

The output of the equaliser is as follows:

$$x_{eq}(t) = \sum_{k=-N}^{N} C_k x(t - kT - NT)$$



The distorted input x(t) has a peak at t = 0 and ISI on each side.

In practice, we will choose the tap gains { C_i } such that

$$x_{eq}(t_k) = \begin{cases} 1 & k = 0 \\ 0 & k = \pm 1, \pm 2, \ldots, \pm N \end{cases}$$

thereby forcing N zero values on each side of the peak of $x_{eq}(t)$. If we apply this constraint, a system of linear equations is created which can be solved to find { C_i }, defining the Zero-Forcing Equaliser with 2N+1 taps.

(d) Based on values that we can calculate from the given pulse shape, the linear system is :-

$$\begin{bmatrix} 1.000 & -0.208 & 0.043 \\ -0.208 & 1.000 & -0.208 \\ 0.043 & -0.208 & 1.000 \end{bmatrix} \begin{bmatrix} C_{-1} \\ C_0 \\ C_1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Forming the equations

$$\begin{aligned} C_{-1} - 0.208C_0 + 0.043C_1 &= 0 \quad (1) \\ -0.208C_{-1} + C_0 - 0.208C_1 &= 1 \quad (2) \\ 0.043C_{-1} - 0.208C_0 + C_1 &= 0 \quad (3) \end{aligned}$$

From (1) and (3) we can see that $C_{-1} = C_1$

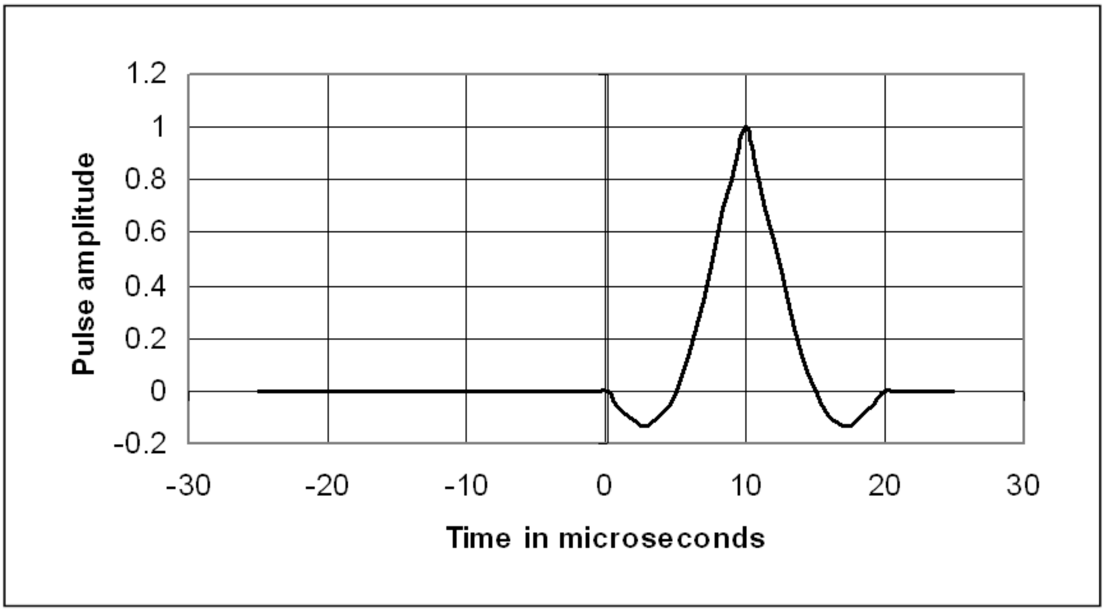
So (2) is $C_0 - 0.416C_1 = 1 \quad (4)$

Subtracting –0.208 times (4) from (1) gives

$$0.956C_1 = 0.208 \Rightarrow C_1 = C_{-1} = 0.218$$

Then in (4) $C_0 = 1 + 0.416 \times 0.2176 = 1.091 \quad (4)$

Calculating the points from $x_{eq}(t) = C_{-1}x(t) + C_0x(t-T) + C_1x(t-2T)$



Q6:

(a) A cipher system has perfect secrecy if the ciphertext gives the cryptanalyst no information about the key. The one time pad achieves perfect secrecy. It comprises a sequence of random numbers known to both the sender and the receiver. A message is encrypted by combining it with an initial segment of the sequence, which is then discarded.

(b) A one-way function is a function that is easy to compute but very difficult to invert. A trapdoor one-way function is a one-way function together with an additional piece of information. Without the extra information the function is very hard to invert but becomes easy to invert with it.

In the case of factorisation, a number c is made by multiplying a×b so that without knowledge of these two numbers we have to factorise c which is a hard problem. Once we know one of the factors, say a, it is trivial to calculate b = c/a.

(c) In a public key cryptosystem separate encryption and decryption keys are used. Each defines a function which is the inverse of the other. Each participant has a public key and a secret key. It is designed to be very difficult to obtain the secret key from the public key or to decrypt a message without the secret key.

It works as follows: suppose Bob wants to send a message to Alice: he obtains her public key, uses this to encrypt his message, and sends it to Alice, who then decrypts the message using her secret key. Anyone can encrypt a message for Alice by using her public key, but no-one can decrypt it without her secret key.

(d) The RSA system relies on the intractability of factorisation compared with the ease of finding large prime numbers. Each participant creates his keys as follows:

1. Select at random two large primes.
2. Compute $n = qr$
3. Select a small odd integer p relatively prime to $\phi(n) = (q-1)(r-1)$.
4. Compute s, the multiplicative inverse of p mod $\phi(n)$.
5. Publish (p,n) as public key.
6. Keep secret (s,n) as secret key.

Messages M are encrypted by $C = M^p \bmod n$.

Ciphertexts C are decrypted by $M = C^S \bmod n$.

To obtain the secret key from the public one the cryptanalyst would need to factor n to obtain q and r and hence $\phi(n)$.

(e) First we need $\phi(n)$

$$\phi(n) = (q-1)(r-1) = 10 \times 6 = 60$$
$$ps = 1(\bmod \phi(n))$$

So $s = \frac{1}{7} \bmod 60 = \frac{61}{7} = \frac{121}{7} = \frac{181}{7} = \frac{241}{7} = \frac{301}{7} = 43 \bmod 60 = 43$