Θέλω να φτιάξω κυκλικό κώδικα
Διαλέγω το μήκος n
Φτιάχνω πολυώνυμο $x^n + 1$
Ορίζω δύο πολυώνυμα $h(x), g(x)$ ώστε $x^n + 1 = h(x)g(x)$

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & ... & g_{n-k} & 0 \\ 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & ... & g_{n-k} \end{pmatrix}$$

$$H = \begin{pmatrix} h_k & h_{k-1} & .. & h_2 & h_1 & h_0 & 0 & 0 & 0 \\ 0 & h_k & h_{k-1} & .. & h_2 & h_1 & h_0 & 0 & 0 \\ 0 & 0 & h_k & h_{k-1} & .. & h_2 & h_1 & h_0 & 0 \\ 0 & 0 & 0 & h_k & h_{k-1} & .. & h_2 & h_1 & h_0 \end{pmatrix}$$

Αν n=7 και $g(x) = (x^3 + x + 1)$ τότε:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Αν θέλω να κωδικοποιήσω το (1101) υπολογίζω το

$$(1101) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = (1010001)$$

$h(x) = x^4 + 0x^3 + x^2 + x + 1$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} (1010001) = (000)$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} (1010000) = (001)$$

$e = (0000001)$
$p = 1/7$
padding:
[message_len 32bit repr,message,padding]
Έστω ότι θέλω να μεταφέρω το 1001

Τρόπος 1ος: (Συστηματικός η λέξη θα υπάρχει στην αρχή της κωδικοποιημένης λέξης)

Βήμα 1: Μετατρέπω τη λέξη σε πολυώνυμο: $m(x) = 1 + x^3$
Βήμα 2: Την πολλαπλασιάζω με το $x^{n-k} = x^{7-4} = x^3$
Βήμα 3: Υπολογίζω $m(x) * x^3 \mod (x^3 + x^2 + 1)$

$(x^3+1)x^3 \mod (x^3+x^2+1) \equiv x^6+x^3 \mod (x^3+x^2+1)$
$\equiv x^2+x+1 \to 111$
1001111

Αποκωδικοποίηση:

Παίρνω τη λέξη που έλαβα πχ 1001111 και την κάνω πολυώνυμο. Ελέγχω αν το πολυώνυμο που έλαβα διαιρείται ακριβώς με το $g(x)$, αν διαιρείται τότε δεν είχες πρόβλημα στην μετάδοση. π.χ.

Αν λάβω 1001111 τότε βρίσκω $m(x) = 1+x^3+x^4+x^5+x^6$

Υπολογίζω το $r(x) = m(x) \mod g(x)$ αν δεν είναι 0 τότε :

$S_i = x^i r(x) \mod g(x)$ και βρίσκω ποιο S_i έχει το μικρότερο βάρος (λιγότερους συντελεστές). Το διάνυσμα λάθους θα είναι:

$x^{n-I} S_I \mod (x^7+1)$