2/15/07

K = GOKNIGHT

G = 47 0100 0111

4 7

K[0] = 0100 K[1] = 0111

S[0] = 0 S[15] = F

T = 4,7, 4,F 4,B, 4E

4,9, 4,7 4,8 5,4

Initialization of S

```
j = 0
for (i=0; i<16, i++)
  { j = (j+S[i]+T[i]) mod16
    swap (s[i], s[j]); }
```

j = 0 + 0 + 4

4, 1, 2, 3, 0, 5, 6, 7 ... 15

FIRST EXAM - 18

4, c, 2, 7, 1, 5, 8, a, 9
d, 0, f, e, 3, b, 6

Stream Generation

```
i = 0
j = 0 , l = 0
for (l = 0, l < P.length, l++)
    i = (i+1) mod 16
    j = (j+1) mod 16
    Swap [ S[i] , S[j] )
    t = ( S[i] + S[j] ) mod 16
    K = S[t]
```

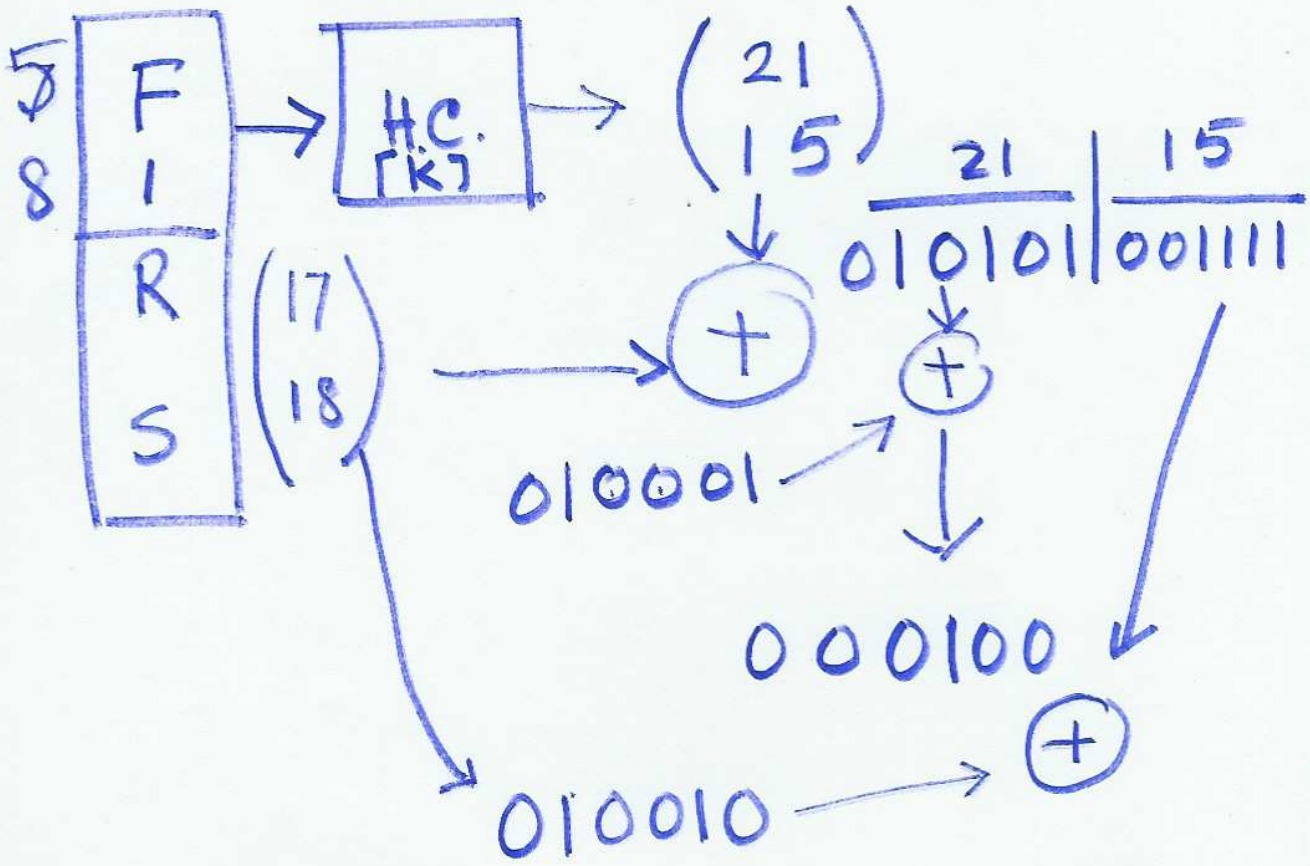
$C(l) = K \oplus P(l)$

Message Integrity Code

FI	RS

6 bits for each character.

$$K = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$$



~~MIC~~ = 000100 011101

000011

T = FIRSTEXAMX

$$K = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}\begin{pmatrix} 5 \\ 8 \end{pmatrix} = \begin{pmatrix} 7\times5+8\times8 \\ 19\times5+3\times8 \end{pmatrix}$$

$$= \begin{pmatrix} 99 \\ 119 \end{pmatrix} = \begin{pmatrix} 21 \\ 15 \end{pmatrix} = \begin{pmatrix} V \\ P \end{pmatrix}$$

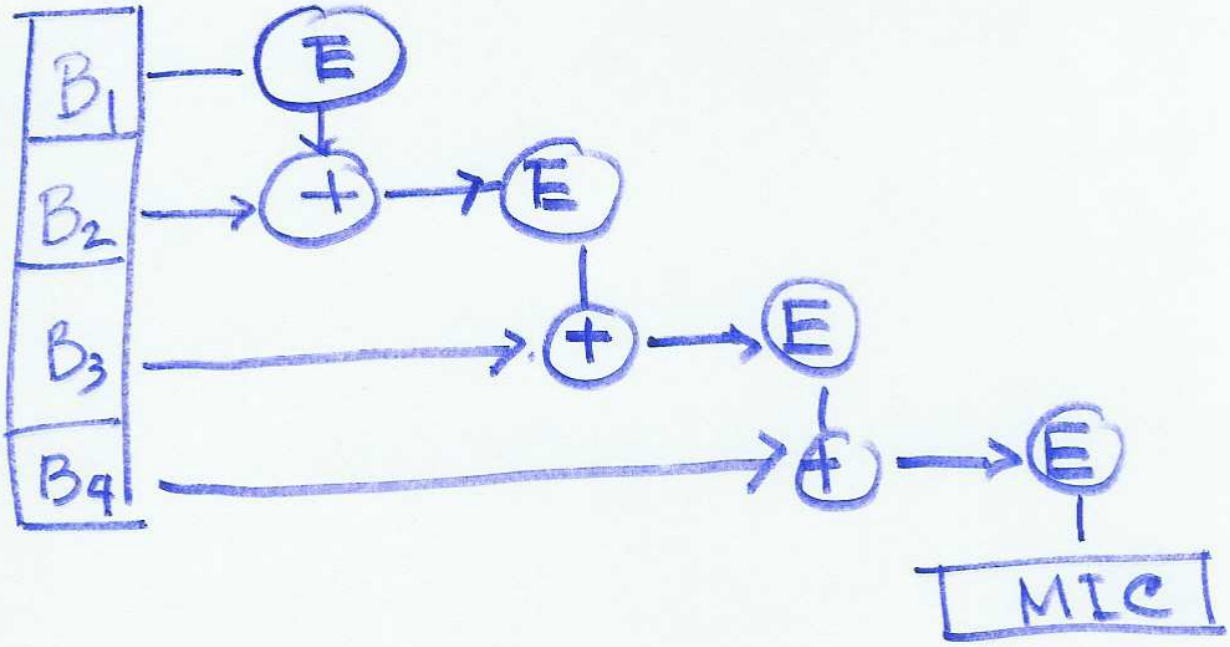
$$\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}\begin{pmatrix} 17 \\ 18 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}\begin{pmatrix} 5 & 17 & 19 & \cdots \\ 8 & 18 & 4 & \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 7X4+8X3 \\ 19X4+3X3 \end{pmatrix}$$

$$= \begin{pmatrix} 52 \\ 85 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \end{pmatrix}$$

MIC = **000000 000111**



TLS

TKIP

CDMA

802.11 a b g