Next extended Eucudean algorithm

$gcd(a,b) = ax+by$

$3 = 93x + 219y$

3 as $27-(6\times4)$

hence $3 = 27 - 4\times6$

sub 6 as $33-(1\times27)$

$\Rightarrow 3 = 27-4\times(33-(1\times27))$

$3 = 27-4\times(33-1\times27)$ sub 27 as $93-(2\times33)$

$= 93-(2\times33)-4\times33+(5\times27)$

$= -4\times33+5\times(93-2\times33)$

$= -14\times33+5\times93$

$= -14\times(219-2\times93)+5\times93$

$= 33(93)+(-14)(219)$

hence $x = 33$ $y = -14$.

$12x+y=2$

$3y=2$

$y=$

$= 3$ as $27-(6+9)$.

$=$

$=$

$y=0$

$3=219y$

$3/219 = 0.013$

$3 = 93x+219(0.013)$

$3 = 93x+2.847$

$93x = 3-2.847$

$x = 0.153/93$

Matrices:

In cryptography, we need to handle matrices. Here we use linear algebra & its uses in cryptography.

$[2 \;\; 5 \;\; 11]$ Row matrix

$\begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}$ column matrix

$\begin{bmatrix} 2 & 3 & 5 \\ 14 & 10 & 11 \\ 30 & 90 & 6 \end{bmatrix}$ Square matrix

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$ Zero matrix

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ Inverse matrix.

Product of row matrix (1×3) by (3×1) will be (1×1)

Ex: $[5 \;\; 2 \;\; 1] \begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix} \Rightarrow (5\times7)+(2\times8)+(1\times2)$

$= 35+16+2$

$= 53$.

Product of 2×3 by 3×4 will be 2×4.

Scalar $= 3\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix}$

$= \begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 3 \end{bmatrix}$.

Determinant is for square matrix.

$\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (5\times4) - (3\times2)$

$= 20 - 6$

$= \underline{14}$ -> determinant.

$\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = 5\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + 2\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + 1\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$

$= 5[0+4] + 2[18+8] + 1[3-0]$

$= 5(+4) + 2(26) + 3$

$= +20 + 46 + 3$

$= \underline{69}$.

Galois Fields

GF(p) is set of integers $\{0, 1, \ldots p-1\}$ with arithmetic operations modulo prime p.

This is finite field.

modular polynomial arithmetic:-

Finite field GF(p)

For given prime P, we have define GF(p) as the set Z_p of integers $\{0, 1, \ldots P-1\}$ together with the arithmetic operations modulo P.

Addition

$$f(x) = a_2x^2 + a_1x + a_0$$

$$g(x) = b_1x + b_0$$

$$f(x) + g(x) = (a_2x^2 + a_1x + a_0) + (b_1x + b_0)$$

$$= a_2x^2 + (a_1 + b_1)x + a_0 + b_0$$

Finite fields are represented by coefficients Z_p such as given as GF(p) notations.

GF(7) where 7 is prime number.

Addition:

$$f(x) = 5x^2 + 4x + 6$$

$$g(x) = 5x + 6$$

$$f(x) + g(x) = [(5x^2 + 4x + 6) + (5x + 6)] \bmod 7$$

$$= (5x^2 + 9x + 12) \bmod 7$$

$$f(x) + g(x) = 5x^2 + 2x + 5$$

Subtraction:

$$f(x) - g(x) = [(5x^2 + 4x + 6) - (5x + 6)] \bmod 7$$

$$= (5x^2 + 4x + 6 - 5x - 6) \bmod 7$$

$$= [5x^2 - x] \bmod 7$$

$$f(x) - g(x) = 5x^2 + 6$$

multiplication:

$$f(x) * g(x) = [(5x^2 + 4x + 6) * (5x + 6)] \bmod 7$$

$$= (25x^3 + 30x^2 + 20x^2 + 24x + 30x + 36) \bmod 7$$

$$= (25x^3 + 50x^2 + 54x + 36) \bmod 7$$

$$f(x) * g(x) = 4x^3 + x^2 + 5x + 1$$

Division

$f(x) = 5x^2+4x+6$

$g(x) = 2x+1$

$2x+1 \overline{)5x^2+4x+6}$

$5/2 = 5 \times (2^{-1}) \bmod 7$

$= 5 \times 4 \bmod 7$

$= 20 \bmod 7$

$= 6.$

first quotent $= 6x$

TO prove

$(2x+1)(6x) \bmod 7$

$= (12x^2+6x) \bmod 7$

$= 5x^2+6x$ (1).

Step 2:- Now subtract $5x^2+6x$ from $5x^2+4x+6$

$(5x^2+6x) - (5x^2+4x+6) \bmod 7$

$= (5x^2+4x+6) - (5x^2+6x) \bmod 7$

$= (5x^2+4x+6-5x^2-6x) \bmod 7$

$= (4x-6x+6) \bmod 7$

$= (-2x+6) \bmod 7$

$= 5x+6$

Step 3:- divid $5x+6$ with $g(x)$

$2x+1 \overline{)5x+6}$

$5/2 = 6x$

second quotient = 6

$\therefore 6x+6$

To prove:

$(6x+6)(2x+1) \bmod 7 = f(x)$

$= (6x+6)(2x+1)$

$= (12x^2+6x+12x+6) \bmod 7$

$= (12x^2+18x+6) \bmod 7$

$= 5x^2+4x+6 = f(x)$

Hence proved.

Block cipher Principles

A stream cipher - encrypts stream of data to converts to the ciphertext.

A Block cipher → encrypts a block of data

It is based on three principles.

→ Number of rounds ✓

→ design of function ✓

→ Key schedule algorithm ✓

Number of rounds:

The number of round judges the strength of Block cipher algorithm. when there is more number of rounds, it is difficult for cryptanalysis to break the algorithm. Even if the function is weak, number of rounds would make the algorithm tough to break.

Design of function F:

Function F of the block cipher, such that is impossible for cryptanalysis to unscramble the situation.

→