Minkovskio konf.

$Z_3[a,b]$ $\quad Z_3 = \{0,1,2\}$ $+, *$ mod 3
$-$ mod 3, $:$ mod 3

$G^+ = \{0,1,2\}$ $\quad G^* = \{1,2\}$

$PP = Q$;

$Q = \{q_{ij}\}$; $\quad i,j \in I_m = \{1,2,\ldots,m\}$

$q_{ij} \in Z_3[a,b]$

Ring of Polynomials $\quad RiP = \langle Z_3[a,b] \mid R_1, R_2, R_3, R_4 \rangle$

R_1: $ab = ba$; $\quad R_2$: $a+b = b+a$;
R_3: $a^2 = a$; $\quad R_4$: $b^2 = b$.

$X = \{x_{ij}\}$; $x_{ij} \in Z_3$ & $Y = \{y_{ij}\}$; $y_{ij} \in Z_3$.

$F_p = \{0,1,2,\ldots,p-1\}$ $\quad p$ – is prime $\quad GF(p^n)$
Q, X, Y are defined over F_p.

STR protocol over the more complicated a.s.

A $\qquad\qquad$ Q $\qquad\qquad$ B

$X \leftarrow$ rand $\qquad\qquad U \leftarrow$ rand

commutation conditions: $X U = U X$

$k \leftarrow$ randi $\qquad$ KAP $\qquad$ $l \leftarrow$ randi

$X Q^k X^{-1} = K_A$ $\quad \rightleftarrows \quad$ $K_B = U Q^l U^{-1}$

$X (K_B)^k X^{-1} = K_{AB} = K = K_{BA} = U (K_A)^l U^{-1}$

$X U \cdot Q^{lk} \cdot U^{-1} X^{-1} = U X Q^{kl} X^{-1} U^{-1}$

$GF(2^{16})$ it is an extention of $GF(2) = F_2 = \{0,1\}$ with primitive polynomial over F_2 of order 17.
If $m = 16$ then the number of matrices Q over $GF(2^{16})$: $N = (2^{16})^{m^2}$

primitive polynomial over F_2 of order 17.

If $m = 16$ then the number of matrices Q over $GF(2^{16})$: $N = (2^{16})^{m^2}$

$$\underbrace{\{1,\ a,\ b,\ ab\}}$$

matix Q consist of elements $GF(2^{16})[a, b]$

It is required to estimate a number of commuting circulant matrices over finite fields.

Let we have a Galois field $GF(2^4)$.

This field consisto $2^4 = 16$ element which are encoded by 4 bits in the following way

0000 0001 0010 0011 0100 - - - - - - . 1111

The multiplication table is a special table depending on the type of primitive pollynomial of 3-rd order over Z_2

$p(t) = 1 + t + t^3 = 1 + 1 \cdot t + 0 \cdot t^2 + 1 \cdot t^3$

1 1 0 1

$GF(2^4)[a, b]$ the examples of this polynomials are:

$0000 + 0101 \cdot a + 1011 \cdot b + 0111 \cdot ab$

$0101 + - - - - - -$

The number of all circulant matrices depends on the number of variats of x_{ij}; $|x_{ij}| = (2^4)^m = 2^{4 \cdot m} = 2^{4 \cdot 32} = 2^{128}$

The number of all matrices Q is equal to

$|q_{ij}|^{m^2}$; $|q_{ij}| = 16^4 = 2^{4 \cdot 4} = 2^{16} = 65536$

$|Q| = (2^{16})^{16} = 2^{256}$.

Security parameters definition and their secure values selection against brute force attack (BFA).

Security parameters are : m - an integer; k, l in bit size

The least security level $Sl = 2^{128}$.

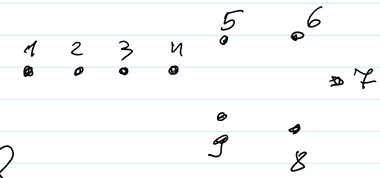
We choose $Sl = 2^{128}$.

Security parameter values: X, U are circulant matrices.

Total number of circulant matrices over Z_3 is 3^m

$|X, U| = 3^m$

Semigroup



Let $m = 16 = 2^4$

Then max k - defines the period of matrix Q

The possible attack is to transform $Z_3[a, b]$ to Cartesian product?

$Q_{a,b} = Q_a \times Q_b$?