VOZES DIVERSAS
DIFERENTES SABERES
CONHECIMENTO FORMAÇÃO INOVAÇÃO
Salão UFRGS 2018
SALÃO DE INICIACAO CIENTIFICA XXX SIC
15 A 19 OUTUBRO CAMPUS DO VALE
UFRGS PROPESQ

Sistema de criptografia Matsumoto-Imai

Bruno Perin Benedetti

Orientadora: Juliane Golubinski Capaverde

Universidade Federal do Rio Grande do Sul - SIC 2018

1- Motivação

O estudo do sistema de Matsumoto-Imai (MI), é muito importante pois nele estão as raízes da grande maioria dos sistemas de criptografia baseados na dificuldade de encontrar soluções para sistemas de equações polinomiais multivariadas. Na apresentação oral, demonstraremos um método utilizado para "quebrar" o sistema MI, denominado "Linearization Equations Attack", esse ataque tem ordem polinomial e, portanto, é aplicável em situações reais.

Outro fator que torna o estudo do sistema MI importante é o fato de ainda não existirem algoritmos quânticos para quebrar as variações avançadas dele. Portanto a existência do computador quântico não invalida esse sistema, o que o torna de certa forma superior aos sistemas baseados na dificuldade de se fatorar inteiros, pois para eles já existe um algoritmo quântico funcional.

2- Construção

Seja k um corpo finito de característica dois e quantidade de elementos q, tome $g(x) \in k[x]$ (anel de polinômios com coeficientes em k) irredutível de grau n. Defina o corpo $K = k[x]/g(x)$ (K é corpo pois g(x) gera um ideal maximal em k[x]).

Definiremos algumas funções para criar o sistema de criptografia.

Seja $\phi : K \longrightarrow k^n$ definida como

$$\phi(a_0 + a_1x + ... + a_{n-1}x^{n-1}) = (a_0, a_1, ... , a_{n-1}).$$

Seja $G : K \longrightarrow K$ definida como

$$G(X) = X^{1+q^{\Theta}} \text{ com } \Theta \text{ tal que } 0 < \Theta < n \text{ e mdc } (q^{\Theta} + 1, q^n - 1) = 1.$$

Logo G é inversível e tem inversa dada por

$$G^{-1}(X) = X^t \text{ com t tal que } t(1+q^{\Theta}) \cong 1 \bmod (q^n - 1).$$

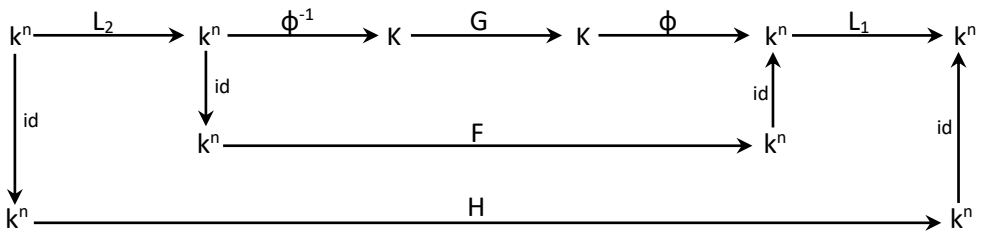
Seja $F : k^n \longrightarrow k^n$ definida como

$$F(x_1, ... , x_n) = \phi \circ G \circ \phi^{-1}(x_1, ... , x_n) = (f_1, ... , f_n).$$

Seja $H: k^n \longrightarrow k^n$ definida como

$H(x_1, ... , x_n) = L_1 \circ F \circ L_2 (x_1, ... , x_n) = (h_1, ... , h_n)$ com L_1 e L_2 duas transformações afim inversíveis em k^n.

Temos o seguinte diagrama:



3- Segurança

Chave Publica:

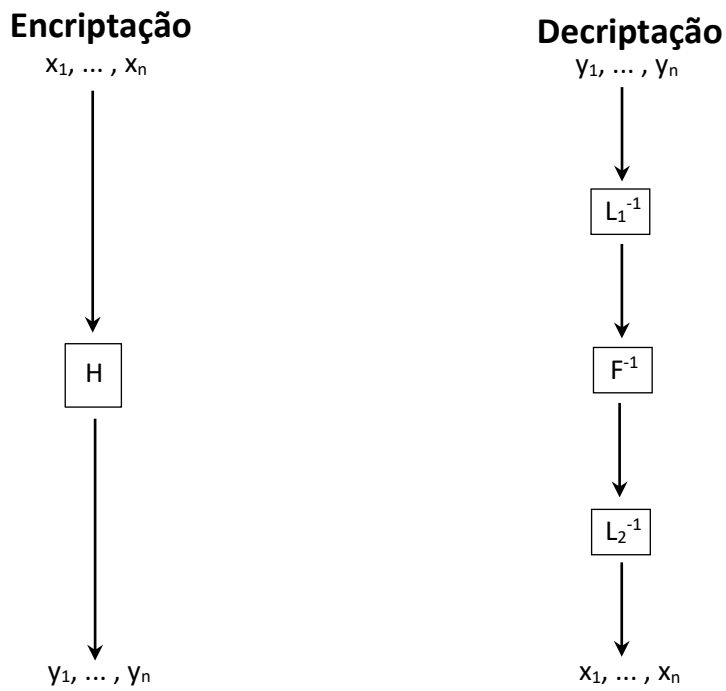
- Corpo k com a estrutura de soma e multiplicação
- Os n polinômios $h_1, ... , h_n \in k[x_1, ... , x_n]$

Chave Privada:

- $L1$ e $L2$ transformações afim inversíveis em k^n
- Pode parecer que Θ tem bastante importância para a segurança do sistema, porém isso não é verdade, portanto ele não é considerado chave privada.

4- Encriptação

A mensagem consiste em $(x_1, ... , x_n) \in k^n$ e a mensagem encriptada $(y_1, ... , y_n) \in k^n$ com $y_i = h_i(x_1, ... , x_n)$, i = 1, ... , n. Diagrama da encriptação e decriptação:



Referência Bibliográfica

Ding, Jintai, Gower, Jason E., e Schmidt, Dieter S. (2006) Multivariate Public Key Cryptosystems