Trabalho de implementação do criptossistema Matsumoto-Imai

Tópicos Especiais em Segurança da Informação - 2017.2 (TCC00230)

Alunos de Graduação:
Bernardo Lopes,
Bruno Gonçalves,
Leandro Almeida

Alunos de Pós-Graduação:
Daniel Bastos

Professor: Luis Kowada

Universidade Federal Fluminense (UFF)

Apresentação

Esta é uma implementação do criptosistema Imai-Matsumoto sem geração automática de chaves públicas. Em vez disso, usamos uma chave pública especifíca com a qual conseguimos exemplificar o sistema. Nossa chave pública de exemplo representa um sistema quadrático de equações não-lineares em cinco dimensões.

Código

A chave privada são as transformações afins Ax + c, Bx + d, o polinômio irredutível f(x) = x^5 + x^4 + x^3 + x + 1, mais os valores h = 9, h' = 7, sendo h h' = 1 mod 31.

Atribuições

No código da classe principal onde se encontra o fluxo principal, primeiramente são feitas as atribuições das variáveis mencionadas acima, além das matrizes A e B e então são computadas suas inversas e os vetores c e d.

Encriptação

A encriptação é meramente y = P(x1, x2, x3, x4, x5), onde P representa o sistema quadrático não-linear. A encriptação está representada na classe principal depois das atribuições das variáveis até a linha 115, quando é produzido o output no console o conteúdo cifrado.

Decriptação

Logo depois começa o código responsável por decapitar a mensagem. Para isso, como Koblitz explica[página 80, 1], usamos dois vetores intermediários, u e v.

Os passos são: v = By + d, onde B é a matriz que representa a transformação /linear/ da transformação afim By + d.

Em seguida precisamos interpretar v como um polinômio porque o próximo passo é elevar v a h'-ésima potência. (E a multiplicação de vetores precisa ser feita exatamente como é feita a multiplicação de polinômios.) Feita a exponenciação, reduzimos o resultado módulo f(x), que é o polinômio irredutível.

Por fim, passamos o vetor resultante da exponenciação pela transformação inversa da transformação afim Ax + c.

Finalmente temos o registro do conteúdo da mensagem decifrado no console.

Referências

[1] Algebraic Aspects of Cryptography (Algorithms and Computation in Mathematics). Neal Koblitz. Springer. 2004. ISBN: 3540634460, 9783540634461.