Universidade Federal do Rio Grande do Sul - UFRGS
Disciplina: Segurança em Sistemas de Computação
Prof. Dr. Jéferson Campos Nobre

Atividade Aula 11

Exercício 1

O algoritmo de criptografia RSA trabalha com números. Dessa forma, para criptografar mensagens de texto, é necessário um método para codificar tal mensagem em números. Um desses métodos é chamado b-adic (onde b é o número de elemento de texto claro) e funciona da seguinte maneira. Suponha que um alfabeto de texto plano consiste dos seguintes elementos:

- <space>ABCDEFGHIJKLMNOPQRSTUVWXYZ ,

ou seja, existe um total de 27 diferentes elementos de texto plano. Assim, os elementos do alfabeto são codificados como segue:

<space> → 0
A → 1
B → 2
...
Z → 26

Dependendo do tamanho de bit do módulo N RSA e o alfabeto selecionado, é possível ajustar o tamanho do bloco utilizado no CrypTool. Assumindo que se quer criptografar o texto plano "MARIO" e que o tamanho do bloco é 2, seriam obtidos os seguintes blocos:

MA#RI#O<space> .

Codificando esses blocos, seria obtido:

13 01 # 18 09 # 15 00 .

Finalmente, b-adic, ou seja, codificação 27-adic de uma representação número da mensagem é obtida através da seguinte fórmula:

<letra 1> × 27 + <letra 2> .

Aplicando esta fórmula, se obtém:

352 # 495 # 405 .

Esta é a sequência de números que será encriptada no texto criptografado (na abordagem “bloco-por-bloco”).

1. Você deve criptografar seu nome usando RSA com um N de pequeno módulo (ou seja, N < 100000). EScolha um N tal que o tamanho do módulo RSA N resultante permita trabalhar com blocos de tamanho 2. No menu principal, em “Crypt/Decrypt” selecione “Asymmetric RSA Demonstration...” para abrir a janela “The RSA Cryptosystem”. Clique em “Options for alphabet and numeric system...” para abrir “Options for RSA Encryption”. Na janela “Options...”, na aba “Alphabet options”, marque “Specify alphabet:”, na aba “RSA variant”, marque “Normal”, na aba “Method for coding a block into numbers”, marque “b-adic”, configure o tamanho do bloco para 2, e finalmente escolha o sistema de numeração “Decimal”. Clique “OK” para salvar as configurações.
2. Demonstre que o sistema de criptografia RSA funciona encriptando o primeiro bloco da mensagem “manualmente”. Para tornar o processo mais simples, use a propriedade “redução por módulo”, que é,

   - $(a \times b) \bmod N \equiv ((a \bmod N) \times (b \bmod N)) \bmod N$

3. Apresente os passos do seu cálculo.
4. Depois de descriptografar o texto criptografado, é preciso decodificar o resultado para a sua representação inicial em texto plano. Como você faria isso?

Exercício 2

"Ciphertext Attack on RSA" é um ataque contra a versão texto do algoritmo RSA. Neste ataque, um atacante primeiro escolhe uma mensagem e a criptografa com a chave pública da vítima. Então, o atacante pede para a vítima assinar (descriptografar) para ele uma mensagem relacionada especialmente construída. Devido a seguinte propriedade do RSA:

- $E(PU, M1) \times E(PU, M2) = E(PU, M1 \times M2)$ (equação 1)

o atacante pode facilmente recuperar qualquer mensagem criptografada com a chave privada da vítima, mesmo sem conhecer tal chave privada. Por exemplo, se o atacante quer descriptografar o seguinte texto cifrado $C = M^e$

mod N, sem conhecer a chave privada *d*. O atacante prossegue da seguinte forma. Conhecendo a chave pública e da vítima, ele prepara a seguinte mensagem:

- $X = (C \times 2^e) \bmod N$

envia a vítima e pede para a mesma assiná-la. A vítima assina a mensagem X com sua chave privada e envia o resultado Y para o atacante

- $Y = X^d \bmod N$

1. Usando Y e a equação 1, o atacante pode recuperar a mensagem criptografada M como segue:

$$\begin{aligned} X^d &= ((C \bmod N) \times (2^e \bmod N))^d \\ &= ((M^e \bmod N) \times (2^e \bmod N))^d \\ &= ((2 \times M)^e \bmod N)^d \\ &= (2 \times M)^{ed} \bmod N \\ &= 2 \times M \end{aligned}$$

2. Mostre com um exemplo que a equação (1) funciona para o RSA. Use o CrypTool para realizar o exemplo. Apresente detalhes da sua solução.

Exercício 3

Este exercício considera o ataque "Factoring Modulus N". Pela fatoração do módulo N RSA, o atacante inicialmente descobre os números primos *p* e *q*. A partir destes, o atacante pode calcular a função Euler $\Phi(N)$ como segue:

- $\Phi(N) = (p - 1)(q - 1)$

além disso, a chave pública e também é conhecida pelo atacante. Logo, ele pode calcular a chave privada correspondente d, a qual é o módulo inverso $\Phi(N)$ de *e*, que é:

- $d = e^{-1} \pmod{\Phi(N)}$

3. Descriptografe a texto cifrado abaixo sabendo que a chave pública e é 11 e o módulo RSA é 40741. O texto claro foi criptografado com tamanho de bloco 2 e codificação 27-adic. Use CryptTool para fatorar o módulo N ("main menu", “Analysis”, “Asymmetric Encryption", "Factorization of a Number...”).

Texto criptografado:
01437 # 32647 # 36721 # 14238 # 24974 # 27041 # 01170 # 31888 #
08891 # 20670 # 07453 # 36364 # 38274 # 06244 # 11809 # 28159 #
12942 # 30673 # 21533 # 12400 # 18298 # 34309 # 36364

Referências

- Baseado em material do Prof. Mario Čagalj (University of Split)