Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 09
Para 18/12/2023

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. Quais são os principais elementos de um criptossistema de chave pública?

2. Quais são os papéis da chave pública e da privada? Descreva-os com detalhes e com exemplos.

3. Quais requisitos os criptossistemas de chave pública precisam cumprir para serem considerados como um algoritmo seguro?

4. Descreva, em termos gerais, um procedimento eficiente para se escolher um número primo.

5. Antes da descoberta de quaisquer esquemas de chave pública específicas, como RSA, uma prova de existência foi desenvolvida, cuja finalidade era demonstrar que a encriptação de chave pública é possível em teoria. Considere as funções $f_1(x_1) = z_1$; $f_2(x_2, y_2) = z_2$; $f_3(x_3, y_3) = z_3$, onde todos os valores são inteiros com $1 \leq x_i, y_i, z_i \leq N$. A função f_1, pode ser representada por um vetor M1 de tamanho N, em que a k-ésima entrada é o valor de $f_1(k)$. De modo semelhante, f_2 e f_3 podem ser representados pelas matrizes M2 e M3 de tamanho $N \times N$. A intenção é indicar o processo de encriptação/decriptação por pesquisas de tabela para aquelas com valores muito grandes de N. Essas tabelas seriam impraticavelmente grandes, mas, a princípio, poderiam ser construídas. O esquema funciona da seguinte forma: construa M1 com uma permutação aleatória de todos os inteiros entre 1 e N; ou seja, cada inteiro aparece exatamente uma vez em M1. Construa M2, de modo que cada linha contenha uma permutação aleatória dos primeiros N inteiros. Finalmente, preencha M3 para satisfazer a seguinte condição:

$$f_3(f_2(f_1(k), p), k) = p \qquad \text{para todo } k, p \text{ com } 1 \leq k, p \leq N$$

Resumindo,

1. M1 toma uma entrada k e produz uma saída x.
2. M2 toma as entradas x e p, dando a saída z.
3. M3 toma as entradas z e k e produz p.

As três tabelas, uma vez construídas, se tornam públicas.

a) Deverá ficar claro que é possível construir M3 para satisfazer a condição anterior. Como um exemplo, preencha M3 para o caso simples a seguir:

$$\text{M1} = \begin{bmatrix} 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{bmatrix} \qquad \text{M2} = \begin{bmatrix} 5 & 2 & 3 & 4 & 1 \\ 4 & 2 & 5 & 1 & 3 \\ 1 & 3 & 2 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{bmatrix} \qquad \text{M3} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ b_1 & b_2 & b_3 & b_4 & b_5 \\ c_1 & c_2 & c_3 & c_4 & c_5 \\ d_1 & d_2 & d_3 & d_4 & d_5 \\ e_1 & e_2 & e_3 & e_4 & e_5 \end{bmatrix}$$

Convenção: o i-ésimo elemento de M1 corresponde a $k = i$. A i-ésima linha de M2 diz respeito $ax = i$; a j-ésima coluna de M2 equivale a $p = j$. A i-ésima linha de M3 indica $z = i$; a j-ésima coluna de MB relaciona-se a $k = j$.

(a) Descreva o uso desse conjunto de tabelas para realizar a encriptação e decriptação entre dois usuários.

(b) Demonstre que esse é um esquema seguro

6. Realize a encriptação e decriptação usando o algoritmo RSA, como na Figura 9.5, para o seguinte:

   (a) $p = 3$; $q = 11$, $e = 7$; $M = 5$;

   (b) $p = 5$; $q = 11$, $e = 3$; $M = 9$;

   (c) $p = 7$; $q = 11$, $e = 17$; $M = 8$;

   (d) $p = 11$; $q = 13$, $e = 11$; $M = 7$;

   (e) $p = 17$; $q = 31$, $e = 7$; $M = 2$.

   Dica: a decriptação não é tão difícil quanto você pensa; use alguma sutileza.

7. Em um sistema de chave pública usando RSA, você intercepta o texto cifrado $C = 10$ enviado a um usuário cuja chave pública é $e = 5$, $n = 35$. Qual é o texto claro M?

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.