Lista 2

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

2013

1. Qual valor de chave do RC4 deixará S inalterado durante a inicialização? Ou seja, após a permutação inicial de S, as entradas de S serão iguais aos valores de 0 até 255 em ordem crescente.
2. Responda as perguntas abaixo:
   (a) Qual é o período máximo que pode ser obtido do seguinte gerador?
   $$x_{n+1} = (aX_n) \mod 2^4$$
   (b) Qual deverá ser o valor de a?
   (c) Que restrições são exigidas na semente?
3. A finalidade deste problema é demonstrar que a probabilidade de que dois números aleatórios sejam relativamente primos é de cerca de 0,6.
   (a) Considere $P = \Pr[\text{mdc}(a,b) = 1]$. Mostre que $\Pr[\text{mdc}(a,b) = d] = \frac{P}{d^2}$. Dica: considere a quantidade mdc $\left(\frac{a}{d}, \frac{b}{d}\right)$.
   (b) Use o resultado acima para determinar o valor de P. Dica: use a igualdade $\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$.
4. Calcule $7^{1000} \mod 10$ utilizando o teorema de Euler (se a e n são relativamente primos, então $a^{\phi(n)} \mod n = 1$).
5. 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?
6. Use o algoritmo de exponenciação rápida para calcular $5^{596} \mod 1234$.
7. Considere um esquema Diffie-Hellman com um primo comum $q = 11$ e uma raiz primitiva $\alpha = 2$.
   (a) Mostre que 2 é uma raiz primitiva de 11.
   (b) Se o usuário A possui chave pública $Y_A = 9$, qual é a chave privada de A, isto é, X_A?
   (c) Se o usuário B em chave pública $Y_B = 3$, qual é a chave secreta compartilhada K,compartilhada com A?
8. É possível usar uma função de hash para construir uma cifra de blocos com uma estrutura semelhante à DES. Se uma função de hash é unidirecional e um bloco cifrado precisa ser reversível (para decriptografia), como isso é possível?

RC4

```
Inicialização(K, keylen)
1. for i=0:255
2.   S(i) ← i
3.   T(i) ← K(i mod keylen)
Permutação Inicial(S, T)
1. j ← 0
2. for i=0:255
3.   j ← (j+S(i)+T(i)) mod 256
4.   Swap(S(i),S(j))
Geração de Fluxo(S)
1. j ← 0
2. i ← 0
3. while true
4.   i ← (i+1) mod 256
5.   j ← (j+S(i)) mod 256
6.   Swap(S(i),S(j))
7.   t ← (S(i)+S(j)) mod 256
8.   k ← S(t)
```

RSA - Rivest-Shamir-Adleman
Geração de Chaves

- Selecione p e q primos e $p \neq q$
- Calcule $n = p \times q$
- $\phi(n) = (p-1) \times (q-1)$, $\phi(n)$ é o tociente de n
- Selecione o inteiro e, tal que $1 < e < \phi(n)$ e $MDC(\phi(n), e) = 1$, isto é, tociente de n e e são relativamente primos
- Calcule $d = e^{-1} \pmod{\phi(n)}$
- Chave pública: $K_{PU} = \{e, n\}$
- Chave privada: $K_{PR} = \{d, n\}$

Criptografia

- Texto claro é um número $M < n$
- Texto cifrado é calculado por $C = M^e \pmod{n}$

Decriptografia

- Texto claro é calculado por $M = C^d \pmod{n}$

Diffie-Hellman

- Elementos públicos globais
  q → número primo
  α → $\alpha < q$ e α é uma raiz primitiva de q
- Geração de chave do usuário A
  (privada) x_A → escolhido tal que $x_A < q$
  (pública) y_A → $y_A = \alpha^{x_A} \mod q$
- Geração de chave do usuário B
  (privada) x_B → escolhido tal que $x_B < q$
  (pública) y_B → $y_B = \alpha^{x_B} \mod q$
- Cálculo da chave secreta
  (privada) K → $K = y_B^{x_A} \mod q = y_A^{x_B} \mod q$