Sub - 24 de Junho de 2013

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

Nome: _____ NUSP: _____

1. **[1.0]** Considere que se deseje criptografar textos com pelo menos 5 bits. Determine um par de chaves pública e privada para criptografar tais textos.
2. **[1.5]** Considere que você intercepte a seguinte chave pública de um servidor $e = 29, n = 143$ e uma mensagem encriptada $C = 56$ utilizando tal chave.
   (a) Determine a chave privada do servidor.
   (b) Determine o texto claro M.
3. **[1.5]** Suponha que você gere uma mensagem autenticada e criptografada aplicando primeiro a transformação RSA determinada por sua chave privada e, depois, cifrando a mensagem por meio da chave pública do destinatário (SEM UTILIZAR HASH). Esse esquema funcionará corretamente, ou seja, permitirá reconstruir a mensagem original no lado do destinatário para todas as relações possíveis entre o módulo n_S do emissor e o módulo n_R do destinatário ($n_S < n_R$, $n_S > n_R$ e $n_S = n_R$)? Explique sua resposta. Caso sua resposta seja 'não', como você corrigiria esse esquema?
4. **[1.5]** Especifique um método para obter números aleatórios inteiros entre 0 e 9 inclusive. Você pode criá-lo ou apresentar um algoritmo já existente. Use o algoritmo para gerar 5 números aleatórios mostrando os passos utilizados.
5. **[1.5]** Os acordos de chaves de Diffie-Hellman e de curvas elípticas, possuem sua força na mesma base teórica. Explique o que há de comum nas duas formas de acordo de chaves.
6. **[1.5]** O protocolo SSL possibilita: integridade e confidencialidade. Explique como ambas características são obtidas no SSL.
7. **[1.5]** Explique a diferença entre IDSs e Firewalls.

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 $M = C^d \pmod{n}$

`EUCLIDES-ESTENDIDO(m,b) : m>b>0`

1. `(A1,A2,A3)` $\leftarrow$ `(1,0,m)`
2. `(B1,B2,B3)` $\leftarrow$ `(0,1,b)`
3. if `B3=0` return `MDC(m,b)=A3` e não existe inverso
4. if `B3=1` return `MDC(m,b)=B3` e $b^{-1} \bmod m = B2$
5. `Q` $\leftarrow \lfloor \frac{A3}{B3} \rfloor$
6. `(T1,T2,T3)` $\leftarrow$ `(A1-Q×B1,A2-Q×B2,A3-Q×B3)`
7. `(A1,A2,A3)` $\leftarrow$ `(B1,B2,B3)`
8. `(B1,B2,B3)` $\leftarrow$ `(T1,T2,T3)`
9. goto `3`