P2 - 27 de Novembro de 2012

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

Nome: _____ NUSP: _____

1. **[1.0]** Considerando o corpo $GF(7)$, encontre o valor de x na equação abaixo. Mostre claramente todos passos utilizados.

$$2x + 3 \pmod 7 = 6x + 5 \pmod 7$$

2. **[1.5]** Realize as seguintes operações polinomiais considerando coeficientes no corpo $GF(5)$.
   (a) $(4x^2 + 3x + 2) + (3x^2 + 2x + 1)$
   (b) $(4x^2 + 3x + 2) - (3x^2 + 2x + 1)$
   (c) $(4x^2 + 3x + 2) \times (3x^2 + 2x + 1)$
   (d) $(4x^2 + 3x + 2) \div (3x^2 + 2x + 1)$
3. **[1.0]** Encontre o inverso multiplicativo de $x^2 + x$ no corpo $GF(2^3)$ utilizando o polinômio irredutível $m(x) = x^3 + x + 1$.
4. **[1.0]** Considere que se deseje criptografar textos com 8 bits. Determine um par de chaves pública e privada para criptografar tais textos.
5. **[1.5]** Considere que você intercepte a seguinte chave pública de um servidor $e = 77, n = 1829$ e uma mensagem encriptada $C = 56$ utilizando tal chave.
   (a) Determine a chave privada do servidor.
   (b) Determine o texto claro M.
6. **[1.0]** Mesmo que utilizar algoritmos de criptografia com chaves longas dificultem a decriptografia, utilizar a mesma chave em textos repetidos podem comprometer a criptografia. Demonstre um esquema de criptografia que utilize números aleatórios para evitar esse problema.
7. **[1.0]** Especifique um método para obter números aleatórios. Você pode criá-lo ou apresentar um algoritmo já existente. Use o algoritmo para gerar 5 números aleatórios.
8. **[1.0]** O protocolo SSL possibilita: integridade e confidencialidade. Explique como ambas características são obtidas no SSL.
9. **[1.0]** 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 $\texttt{b}^{-1}\text{mod}\,\texttt{m}=\texttt{B2}$
5. `Q` $\leftarrow \lfloor \frac{\texttt{A3}}{\texttt{B3}} \rfloor$
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`