Sub - 24 de Junho de 2013

ACH2076 - Segurança da Informação (Valdinei Freire da Silva)

Nome: _____ NUSP: _____

1. **[1.0]** Uma forma de avaliar a força de uma criptografia é mensurar a distribuição de letras (bytes, words, etc.) no texto cifrado. Idealmente as características do texto aberto devem ser escondidas no texto cifrado, por exemplo, gerando um texto cifrado com distribuição uniforme das letras. Considerando a cifra de Vigenère, especifique as condições necessárias que uma chave deve ter para garantir distribuição uniforme no texto cifrado.
2. **[1.0]** Uma desvantagem da cifra monoalfabética é que quem envia a mensagem e quem recebe a mensagem devem guardar na memória uma senha de 26 caracteres. Uma técnica comum para evitar isso é utilizar uma chave menor, e gerar uma chave monoalfabética a partir da mesma.
   Por exemplo, usando a chave CIPHER, primeiro escreva a chave na primeira linha e escreva as letras restantes nas linhas sucessivas, obtendo:

   ```
   C  I  P  H  E  R
   A  B  D  F  G  J
   K  L  M  N  O  Q
   S  T  U  V  W  X
   Y  Z
   ```

   Agora gere uma sequência de letras lendo as colunas de cima para baixo e da direita para esquerda, obtendo a chave monoalfabética:

   `CAKSYIBLTZPDMUHFNVEGOWRJQX`

   Considerando o esquema acima, o texto aberto "`os alunos deveriam ser mais participativos na aula`" foi cifrado obtendo o texto "`DR VQAZDR LPFPNCVU RPN UVCR EVNWCGCEVWCFDR ZV VAQV`". Encontre as quatro possíveis chaves utilizadas.
   Dica: trabalhe com a posição da letra `A` para teorizar sobre o tamanho da palavra chave.
3. **[1.0]** A forma mais simples de ataque a cifras considera pares (texto claro - texto cifrado) escolhidos arbitrariamente. Considerando a cifra de Hill, quais são as condições que esses pares devem apresentar? Qual é a quantidade mínima de pares de textos?
4. **[1.0]** Outra forma de ataque é a força bruta. Nesse caso, todas as chaves são testadas e a que produz um texto mais inteligível é considerada a chave correta. Considerando as características da cifra de Hill, esquematize alguma estratégia para reduzir a quantidade de chaves testadas em um ataque a essa cifra.
5. **[2.0]** Duas estratégias de cifras utilizadas para produzir cifras fortes são: cifras de Feistel e redes de Substituição-Permutação. Responda às perguntas abaixo:
   a) Especifique a fórmula para uma rodada da cifra de Feistel?
   b) Especifique a fórmula para uma rodada da rede da Substituição-Permutação?
   c) Em ambos casos, qual é a máxima entropia (média) obtida após uma única rodada? Explique.
6. **[1.0]** Encontre o inverso multiplicativo do número 300 no corpo $GF(503)$.
7. **[1.0]** Monte a tabela de multiplicação do número 5 no corpo $GF(11)$ e indique o inverso multiplicativo e aditivo para 5.
8. **[1.0]** Monte a tabela de multiplicação do número 6 no corpo $GF(3^2)$ e indique o inverso multiplicativo e aditivo para 6. Utilize o polinômio irredutível $2x^2 + 2$.
9. **[1.0]** Cite três diferenças fundamentais entre as cifras AES e DES.

`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`$\times$`B1,A2-Q`$\times$`B2,A3-Q`$\times$`B3)`
7. `(A1,A2,A3)` $\leftarrow$ `(B1,B2,B3)`
8. `(B1,B2,B3)` $\leftarrow$ `(T1,T2,T3)`
9. goto `3`