Examen

Carlos Javier Alonso Caldera

1.- Responder las siguientes preguntas

a) ¿Cual de los metodos de cifrado revisados en el recorrido historico considera mas ingenioso y por que?

R= Se me hace muy interesante el cifrado vigénere por el tamaño de la tabla y como se debe de fragmentar el mensaje con la longitud de la llave

b) ¿Que significa que un metodo de cifrado sea de sostitucion policalfabetica? R= Aquellos que hacen el uso de varios alfabetos para cifrar el mensaje

c) En el cifrado de Playfair la matriz utilizada tiene en la misma posicion los caracteres "i" y "j".

Describa detalladamente la forma en la que esta sostitucion puede afectar al proceso de cifrado o desifrado R= Realmente no creo que afecte mucho en rendimiento ni en error en el mensaje ya que solo a sostituir "i" o "j" en el mensaje final

2.- Describe sin ambiguedades la relacion existente entre los conceptos "entropia", "Cantidad de informacion" e "incertidumbre" R= La entropia o la cantidad de informacion en un mensaje y la incertidumbre es la probabilidad de obtener una parte de informacion o otra parte.

3: Suponga el siguiente escenario: Se tiene una caja con capacidad para almacenar 10 bolsas y usted es libre de elegir los colores de la bolsa a introducir. ¿Cual seria la configuracion del escenario para que la entropia del sistema sea la maxima para el cuento "sacar una bolsa"?

Al preguntar por si cual es la configuracion, se refiere a que indique los colores de las bolas a introducir por ejemplo: 5 negras y 5 blancas, o 3 negras, 3 blancas y 4 azules, etc

R= 10 bolas distintas para tener una incertidumbre alta y una entropia alta

$$H(x) = -(1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10) + (1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10) + 1/10 \log_2(1/10)))$$

$$H(x) = -(0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1) + 0.1 \log_2(0.1))$$

$$H(x) = -(-0.33 - 0.33 - 0.33 - 0.33 - 0.33 - 0.33 - 0.33 - 0.33 - 0.33 - 0.33)$$

$$H(x) = 0.33 + 0.33 + 0.33 + 0.33 + 0.33 + 0.33 + 0.33 + 0.33 + 0.33 + 0.33$$

$$H(x) = 3.3$$

4: En la prueba de primalidad de Fermat, para asegurar que numero es compuesto, se verifica si $a^{(n-1)}$ no es congruente con $1 \pmod n$. Indique un par de numeros "a" y "n" que ejemplifiquen el flujo del programa que se retorne "Compuesto" Para comprobar realice la congruencia mencionada en la condicion.

$a = 2 \quad n = 9$

$2^{(9-1)} \bmod 9 \neq 1 \bmod 9$

$2^8 \bmod 9 \neq 1 \bmod 9$

$256 \bmod 9 \neq 1 \bmod 9$

$7 \neq 1 \rightarrow$ Compuesto

5 Resolver el siguiente sistema de congruencias mediante el teorema chino de residuo, realizando de manera explicita paso a paso cada seccion que se requiera (los inversos obtenerlos mediante el algoritmo extendido de Euclides)

b.

$x = 1 \mod 3$

$x = 2 \mod 5$

$x = 3 \mod 11$

$x = 4 \mod 7$

① modulos

$m = 3 \cdot 5 \cdot 11 \cdot 7$

$m = 1,155$

② $C_i = \frac{M}{n_i}$

$C_1 = \frac{1,155}{3} = 385$ $C_2 = \frac{1,155}{5} = 231$ $C_3 = \frac{1,155}{11} = 105$ $C_4 = \frac{1,155}{7} = 165$

③ d_i = inverso de $c_i \mod n_i$

d_1 = inverso de 385 mod 3 = 1

d_2 = inverso de 231 mod 5 = 1

d_3 = inverso de 105 mod 11 = 2

d_4 = inverso de 165 mod 7 = 2

d_1 = inverso de 385 mod 3

$385 = 3 \cdot 128 + 1$

$3 = 1 \cdot 3 + 0$

Despejar

(1) $385 - 3 \cdot 128 = 1$

inverso = 1

d_2 = inverso de 231 mod 5

$231 = 5 \cdot 46 + 1$

$5 = 1 \cdot 5 + 0$

Despejar

(1) $231 - 5 \cdot 46 = 1$

inverso = 1

d_3 = Inverso de 105 mod 11

$105 = 11 \cdot 9 + 6$

$11 = 6 \cdot 1 + 5$

$6 = 5 \cdot 1 + 1$

$5 = 1 \cdot 5 + 0$

Despejar

$105 - 11 \cdot 9 = 6$

$11 - 6 \cdot 1 = 5$

$6 - 5 \cdot 1 = 1$

$1 = 6 - 5 \cdot 1$

$1 = 6 - (11 - 6 \cdot 1) \cdot 1$

$1 = 6 - 11 + 6$

$1 = 2(6) - 1(11)$

$1 = 2(105 - 11 \cdot 9) - 1(11)$

$1 = 2(105) - 2(11 \cdot 9) - 1(11)$

$1 = 2(105) - 18(11) - 1(11)$

$1 = 2(105) - 19(11)$

residuo = 2

d_4 = inverso de 165 mod 7

$165 = 7 \cdot 23 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

Despeje

$165 - 7 \cdot 23 = 4$

$7 - 4 \cdot 1 = 3$

$4 - 3 \cdot 1 = 1$

$1 = 4 - 3 \cdot 1$

$1 = 4 - (7 - 4 \cdot 1) \cdot 1$

$1 = 4 - 7 + 4$

$1 = 2(4) - 7$

$1 = 2(165 - 7 \cdot 23) - 7$

$1 = 2(165) - 2(7 \cdot 23) - 7$

$1 = 2(165) - 46(7) - 7$

$1 = 2(165) - 47(7)$

Inverso = 2

④ Solucion = $\hat{\sum_{i=1}}$ bi ci di

$= (1 \cdot 385 \cdot 1) + (2 \cdot 231 \cdot 1) + (3 \cdot 100 \cdot 2) + (4 \cdot 165 \cdot 2)$

$= 385 + 462 + 630 + 1320$

$= 2,797 \bmod 1,155$

$= 487$