Universidad Nacional Autónoma de México
Facultad de Ciencias - Ciencias de la Computación
Criptografía y seguridad 2019-2

Tarea 1

25 de febrero de 2019

Fecha límite de entrega: 19 de marzo a las 11:00 am.
Equipos de hasta 3 personas.

1. *a*) Supón que en un criptosistema se tiene $\#\mathcal{M} = \#\mathcal{C}$. Demuestra que para cualquier llave $k \in \mathcal{K}$ y cualquier criptotexto $c \in \mathcal{C}$, existe un único mensaje claro $m \in \mathcal{M}$ tal que $\mathsf{Enc}_k(m) = c$.

   b) Sea $S_{m,c} = \{k \in \mathcal{K} : \mathsf{Enc}_k(m) = c\}$, es decir, el conjunto de llaves que encriptan m en c. Demuestra que para distintos c, c' se tiene $S_{m,c} \cap S_{m,c'} = \emptyset$.

2. Alicia y Bartolo escogen un espacio de claves $\mathcal{K}$ que contiene 2^{56} claves. Supón que Eva tiene una computadora que puede revisar 10^{10} claves por segundo.

   a) ¿Cuántos días le tomaría a Eva revisar todas las claves de $\mathcal{K}$?

   b) Si Alicia y Bartolo cambian su esquema por uno con un conjunto más grande, con 2^B claves, ¿qué tan grande debe ser B para que la computadora de Eva tarde 100 años revisando todas las claves? (Puedes suponer que un año tiene 365.25 días.)

3. Combina las siguientes parejas de números usando la operación de XOR ($\oplus$) a nivel de bits.

   a) Cadenas de bits: 1100110010, 0100010001.

   b) Números decimales: 8191, 16383.

   c) Cadenas de bytes: `0x23ab873f`, `0x1a003dfb`. (Los símbolos `0x` solo son para indicar que es hexadecimal.)

4. ¿Los siguientes esquemas de cifrado son perfectamente seguros? Explica.

   a) Los mensajes claros son $\mathcal{M} = \{0, 1, \ldots, 9\}$. El algoritmo Gen devuelve una clave al azar del conjunto $\mathcal{K} = \{0, 1, \ldots, 13\}$. La función $\mathsf{Enc}_k(m)$ calcula $(k + m)$ mód 10, y $\mathsf{Dec}_k(c)$ devuelve $(c - k)$ mód 10.

   b) $\mathcal{M} = \{m \in \{0,1\}^\ell \mid \text{el último bit de } m \text{ es } 0\}$. Gen escoge una clave aleatoria de $\{0,1\}^{\ell-1}$. $\mathsf{Enc}_k(m)$ devuelve $m \oplus (k||0)$, y para descifrar $\mathsf{Dec}_k(c)$ devuelve $c \oplus (k||0)$. (El símbolo $||$ denota concatenación.)

   c) El algoritmo de desplazamiento para mensajes de tamaño uno sobre el alfabeto `ABC...Z` de 26 letras.

5. Sea Π el esquema de Vigenère, donde $\mathcal{M} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}^3$, la clave se genera escogiendo aleatoriamente un número $t \in \{1, 2, 3\}$ y luego se escoge una clave aleatoria de tamaño t.

   Un adversario $\mathcal{A}$ entrega $m_0 = \mathtt{aab}$ y $m_1 = \mathtt{abb}$. Cuando se le da un texto cifrado $c = c_1c_2c_3$, devuelve 0 si $c_1 = c_2$ y 1 en caso contrario. Calcula $\Pr[\mathsf{PrivK}_{\mathcal{A},\Pi} = 1]$.

6. Considera el criptosistema de sustitución monoalfabética con los siguientes cambios: $\mathcal{M} = \mathcal{C} = \text{ALF}^\ell$, es decir, los mensajes son cadenas de tamaño ℓ sobre el alfabeto ALF, y $\mathcal{K} = P^\ell$, donde

P es el conjunto de permutaciones de ALF, es decir, una llave $k = k_1, \ldots, k_\ell$ corresponde a ℓ permutaciones de ALF. La función de cifrado se define como

$$\mathsf{Enc}_k(m) = k_1(m_1), k_2(m_2), \ldots, k_\ell(m_\ell) \quad \text{donde } m = m_1, \ldots, m_\ell,\ k = k_1, \ldots, k_\ell$$

a) ¿Cómo se define $\mathsf{Dec}_k(c)$?

b) Demuestra que este criptosistema es perfectamente seguro.

7. Definimos Π como una versión modificada de one-time pad, donde $\mathcal{M} = \{0,1\}^\ell$, pero ahora $\mathcal{K}$ son las cadenas de ℓ bits con un número par de unos; el cifrado y descifrado son iguales que en one-time pad. Construye un adversario $\mathcal{A}$ tal que $\Pr[\mathsf{PrivK}_{\mathcal{A},\Pi} = 1] = 1$.

8. Sea Π un esquema de cifrado perfectamente seguro con un espacio de llaves $\mathcal{K} = \{0,1\}^\ell$. Supongamos que un banco desea partir una llave k en tres partes p_1, p_2, p_3 de forma que para poder descifrar es necesario usar dos de las tres partes. De esta forma, cada parte se le entrega a un ejecutivo distinto, y el descifrado solo es posible si se juntan al menos dos de los tres ejecutivos.

   Inicialmente el banco genera aleatoriamente dos pares de llaves (k_1, k_1') y (k_2, k_2') que satisfacen la relación
$$k_1 \oplus k_1' = k_2 \oplus k_2' = k,$$
   y al primer ejecutivo se le asigna la parte $p_1 = (k_1, k_2)$.

   a) Define las partes p_2 y p_3 para que cumplan la condición deseada, es decir, que con cualesquiera dos partes se puede recuperar k, pero con una sola no es posible.

   b) Haz los cambios necesarios en el esquema anterior, de forma que ahora se necesiten 3 de 5 partes para poder descifrar. (Y con dos partes no se obtiene información sobre k.)

9. Considera el siguiente escenario sobre una votación. Se tienen t votantes, y cada uno puede votar 0 o 1. Al final de la votación una persona anuncia el resultado S, que corresponde a la suma de todos los votos. Para llevar a cabo la votación de forma que ningún votante sepa nada más que el resultado S, se propone el siguiente protocolo.

   Sea $n > t$ un entero. Al inicio de la votación el encargado genera $c_0 \xleftarrow{\$} \{0, 1, \ldots n-1\}$. El primer votante recibe c_0 y obtiene $c_1 = c_0 + v_1 \bmod n$, donde $v_1 \in \{0,1\}$ es su voto. Luego le pasa c_1 al votante 2 y este hace lo análogo. Sucesivamente, el votante i recibe el valor c_{i-1}, calcula $c_i = c_{i-1} + v_i \bmod n$ y se lo entrega al votante $i+1$. El votante t obtiene c_t y se lo entrega al encargado, este último calcula $S = c_t - c_0 \bmod n$ y lo anuncia a todos los votantes.

   a) Muestra que el encargado al final efectivamente calcula la suma de todos los votos.

   b) Suponiendo que en el protocolo los votantes se comportan honestamente, al final de la votación cada votante i solo es capaz de conocer S y el valor c_{i-1} (además del propio voto v_i); definimos $Vista_i = (S, c_{i-1})$. Si fijamos los valores de i y S, el votante i puede tener distintas vistas $Vista_i$, dependiendo de cómo fueron los votos de los demás votantes.

   ¿Los diferentes valores posibles de $Vista_i$ sirven para que el votante i pueda distinguir el voto de otro votante? ¿Por qué?

   c) Supón que dos votantes deshonestos quieren conocer el voto de un tercero. ¿Cómo pueden lograrlo? (Sin usar el método del garrote.)