Criptografía: Aspectos Teóricos y Prácticos — Práctico 1

1. Sean N, g y A enteros positivos. Probar que el siguiente algoritmo, que es una variante del algoritmo de *elevar al cuadrado y multiplicar* explicado en la clase práctica, devuelve el valor $g^A \mod N$.

Algoritmo 1 Variación de *elevar al cuadrado y multiplicar*

Require: Enteros positivos N, g y A.
Ensure: El valor de $g^A \mod N$.

```
a ← g, b ← 1
while A > 0 do
    if A ≡ 1 mód 2 then
        b ← b · a mód N
    end if
    a ← a^2 mód N, A ← ⌊A/2⌋
end while
return b
```

   Este algoritmo requiere almacenar menos datos que el algoritmo de *elevar al cuadrado y multiplicar*. ¿Por qué?

2. Sea p un primo tal que $q = \frac{p-1}{2}$ es primo. Sea g un entero tal que

   - $g \neq \pm 1 \mod p$,
   - $g^q \neq 1 \mod p$.

   Probar que g es una raíz primitiva módulo p.

3. Sea p un primo, y sea q un primo que divide a $p-1$.

   a) Sean $a \in \mathbb{F}_p^*$ y sea $b = a^{\frac{p-1}{q}}$. Probar que o bien $b = 1$ o bien b tiene orden q.

   b) Supongamos que buscamos un elemento de $\mathbb{F}_p^*$ de orden q. Usando el ítem anterior, podemos elegir aleatoriamente elementos $a \in \mathbb{F}_p^*$ y chequear si $b = a^{\frac{p-1}{q}}$ satisface $b \neq 1$. ¿Qué probabilidades tenemos de tener éxito? En otras palabras, calcular el cociente

$$\frac{\#\left\{a \in \mathbb{F}_p^* : a^{\frac{p-1}{q}} \neq 1\right\}}{p-1}.$$

4. Desencriptar el siguiente mensaje, sabiendo que ha sido encriptado utilizando un cifrado de sustitución simple, y que el texto plano está escrito en inglés. El texto se puede encontrar en la página EVA.

```
JNRZR BNIGI BJRGZ IZLQR OTDNJ GRIHT USDKR ZZWLG OIBTM NRGJN IJTZJ
LZISJ NRSBL QVRSI ORIQT QDEKJ JNRQW GLOFN IJTZX QLFQL WBIMJ ITQXT
HHTBL KUHQL JZKMM LZRNT OBIMI EURLW BLQZJ GKBJT QDIQS LWJNR OLGRI
EZJGK ZRBGS MJLDG IMNZT OIHRK MOSOT QHIJL QBRJN IJJNT ZFIZL WIZTO
MURZM RBTRZ ZKBNN LFRVR GIZFL KUHIM MRIGJ LJNRB GKHRT QJRUU RBJLW
JNRZI TULGI EZLUK JRUST QZLUK EURFT JNLKJ JNRXR S
```

5. Considerar el cifrado afin dado por un primo p y la clave $k = (k_1, k_2) \in \mathbb{F}_p^* \times \mathbb{F}_p$. Es decir, la función de cifrado $e_k : \mathbb{F}_p \to \mathbb{F}_p$ está dada por $e_k(m) \equiv k_1 \cdot m + k_2 \mod p$.

a) Sean $p = 541$ y $k = (34, 71)$. Encriptar el mensaje $m = 204$. Desencriptar el texto cifrado $c = 431$.

b) Alicia y Beto deciden utilizar el primo $p = 601$ para su cifrado afín, lo cual es de público conocimiento. Eva logra averiguar que los mensajes $m_1 = 387$ y $m_2 = 491$ son encriptados como $c_1 = 324$ y $c_2 = 381$. Hallar la clave privada.

c) Suponiendo que p es de público conocimiento, explicar por qué el cifrado afín es vulnerable a un ataque de texto plano elegido. ¿Cuántos pares (texto plano, texto cifrado) se necesitan para recuperar la clave privada?

d) Si p no es de púbico conocimiento, ¿es el cifrado afín vulnerable a un ataque de texto plano elegido? En caso afirmativo, ¿cuántos pares (texto plano, texto cifrado) se necesitan para recuperar la clave privada?

6. Sean N un entero positivo, y sean $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}/N\mathbb{Z}$. Consideremos las funciones $e : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ dadas por

   a) $e_k(m) \equiv k - m \mod N$,

   b) $e_k(m) \equiv k \cdot m \mod N$,

   c) $e_k(m) \equiv (k + m)^2 \mod N$.

   En cada caso, decidir si e es una función de cifrado. En caso negativo, justificar por qué. En caso afirmativo, hallar la función de descifrado.

7. El cifrado *one-time pad* de Vernam está dado por la función $e_k(m) = k \oplus m$, donde k y m son cadenas de bits de la misma longitud, y la operación $\oplus$ está dada por aplicar XOR lugar a lugar.

   a) Hallar la función de desencriptado.

   b) Mostrar que este cifrado es vulnerable a un ataque de texto plano elegido. Hallar la clave privada usada por Alicia y Beto, sabiendo que el texto plano $m = 0010010000101100$ se encripta como $c = 1001010001010111$.

   c) ¿Qué sucede si se utiliza el cifrado más de una vez?

8. Supongamos que Alicia y Beto consideran la función de encriptado $e_p : \mathbb{Z} \to \mathbb{Z}$ dada por $e_p(m) = p \cdot m$, donde p es un número primo que sólo ellos conocen. Si Eva intercepta los textos cifrados $c_1 = 12849217045006222$ y $c_2 = 6485880443666222$, entonces calculando el máximo común divisor entre c_1 y c_2 puede hallar p. ¿Cómo lo hace? ¿Quién es p? ¿Quiénes son m_1 y m_2?

En este curso la expectativa es que cada estudiante trabaje alrededor de 7 horas en cada práctico. Como es la primera que lo dictamos, no sabemos cuánto tiempo tomará esta lista de ejercicios. Así que te pedimos que nos des una idea de cuánto tiempo te demoró hacerla (sin contar el tiempo invertido en Facebook, Whatsapp, etc.).