Práctica 3: Construcción de un criptosistema

Erik Altelarrea Ferré

Criptografía (UOC). Mayo 2022

1 Análisis criptográfico del cifrado

1. Teniendo en cuenta que si $n = p_1^{r_1} \cdots p_l^{r_l}$, donde $p_1, ..., p_l$ son números primos, entonces $\phi(n) = (p_1 - 1) \cdots (p_l - 1)p_1^{r_1 - 1} \cdots p_l^{r_l - 1}$, calcula el orden del grupo $\mathbb{Z}_{N^2}$.

Usaremos que $N = pq$, de manera que $N^2 = p^2q^2$. Luego $\phi(N^2) = (p-1)(q-1)pq = (p-1)(q-1)N$ es el orden del grupo $\mathbb{Z}_{N^2}$.

2. Calcula, para todo a tal que $mcd(a, N) = 1$, $a^{N(p-1)(q-1)} \mod N^2$.

Aplicaremos el Teorema de Euler, que afirma que dados n un número natural, $\phi(n)$ su función fi de Euler y x tal que $mcd(x, n) = 1 \implies x^{\phi(n)} = 1 \mod n$. Observamos, además, que $mcd(a, N) = 1 \implies mcd(a, N^2) = 1$.

Del ejercicio anterior sabemos que $\phi(N^2) = N(q-1)(p-1)$, como $a^{N(p-1)(q-1)} = a^{\phi(N^2)}$, aplicando el Teorema de Euler, tenemos que $a^{N(p-1)(q-1)} \equiv 1 \mod N^2$.

3. Utiliza el apartado anterior para demostrar que $c^d = 1 + mN \mod N^2$.

Por definición, sabemos que $c = (1+N)^m r^N \mod N^2$ donde $m \in \mathbb{Z}_m$ y $r \in \mathbb{Z}_N^*$. $r \in \mathbb{Z}_N^* \implies mcd(r, N) = 1 \implies mcd(r, N^2) = 1$, de manera que, por el Teorema de Euler, $r^{\phi(N^2)} \equiv 1 \mod N^2$. También, sabemos que $d \equiv 1 \mod N$ y $d \equiv 0 \mod (p-1)(q-1)$, lo que se traduce en $d - 1 = tN$ y $d = k(p-1)(q-1)$ para ciertos $t, k \in \mathbb{Z}$.

Así, $c^d = (1+N)^{md} r^{Nd} = (1+N)^{md} r^{Nk(q-1)(p-1)} = (1+N)^{md} (r^{N(q-1)(p-1)})^k = (1+N)^{md} (r^{\phi(N^2)})^k \equiv (1+N)^{md} 1^k \mod N^2 \equiv (1+N)^{md} \mod N^2 \equiv (1+N)^{m(1+tN)} \mod N^2$.

Llegados a este punto, ya sabemos que $c^d \equiv (1+N)^{m(1+tN)} \mod N^2$. Veamos, finalmente, que $(1+N)^{m(1+tN)} \equiv 1 + mN \mod N^2$. Para ello emplearemos el binomio de Newton para desarrollar la potencia $(1+N)^{m(1+tN)}$:

$$(1+N)^{m(1+tN)} = \sum_{k=0}^{m(1+tN)} \binom{m(1+tN)}{k} 1^{m(1+tN)-k} N^k = \sum_{k=0}^{m(1+tN)} \binom{m(1+tN)}{k} N^k =$$

$$= 1 + m(1+tN)N + \frac{m(1+tN)tN}{2} N^2 + \frac{m(1+tN)tN(tN-1)}{6} N^3 + ... + N^{m(1+tN)}$$

$$\equiv 1 + m(1+tN)N \mod N^2 \equiv 1 + mN + mtN^2 \mod N^2 \equiv 1 + mN \mod N^2$$

donde se ha usado que $N^k \equiv 0 \mod N^2 \ \forall k \geq 2$.

2 Sistema de votación

1. Dados c_1 y c_2 dos textos cifrados de m_1 y m_2 respectivamente, ¿cuál es el mensaje en claro del texto cifrado c_1c_2?

El mensaje en claro es $m_1 + m_2$.

2. Bob decide utilizar esta propiedad para diseñar un sistema de votación. Así, suponiendo que los votos son $m = 1$ (SI) o $m = 0$ (NO), ¿cómo puede calcular el resultado de la votación a partir de los votos, si estos están cifrados con la cifra anterior?

Bob puede limitarse a calcular el producto de todos los votos recibidos, y aplicar el algoritmo de descifrado al resultado de dicho producto. Este resultado será la cantidad de votos SI. Para hallar la cantidad de votos NO, Bob puede calcular la diferencia entre el número de votos recibidos y el número de votos SI.

4. Explicad qué ventajas o inconvenientes tiene, desde el punto de vista de la privacidad, utilizar un sistema como el descrito en el apartado anterior.

Observamos que para cifrar cada voto únicamente es necesario saber el valor de N, la clave pública, mientras que para descifrar, es necesario conocer tanto N como d.

Esto hace que no sea posible asociar un voto cifrado a la persona que lo emite, garantizando así la privacidad del votante. Al emitirse el voto cifrado, se garantiza además la privacidad del voto.

No obstante, no hay ningún control acerca del número de veces que vota cada votante. Ello es una clara desventaja puesto que una misma persona puede votar un número indefinido de veces sin que el criptosistema lo detecte.

Además, emisor y receptor deberán compartir el valor N de forma segura. De lo contrario, toda la comunicación será vulnerable a ataques dado que cualquiera puede emitir un voto conociendo únicamente el valor de N.