Criptografía y Seguridad Computacional - IIC3253
Tarea 2
Solución pregunta 1

En esta pregunta usted va a implementar y demostrar la corrección de un esquema criptográfico que utiliza claves más simples que las de RSA, y que además es aleatorizado, produciendo con una alta probabilidad cifrados distintos si un mensaje es encriptado más de una vez.

Para definir este esquema, necesitamos introducir un poco de notación. Dado un número natural n, sea $\#\text{Bit}(n)$ el número de bits en la representación binaria de n. Además, dados dos números naturales n, m tales que $m > 0$, sea

$$\text{Div}(n, m) \quad = \quad \left\lfloor \frac{n-1}{m} \right\rfloor.$$

Entonces, la clave pública P_A y la clave secreta S_A de un usuario A son generadas de la siguiente forma.

(a) Genere dos números primos distintos P y Q tales que $P \geq 3$, $Q \geq 3$ y $\#\text{Bit}(P) = \#\text{Bit}(Q)$. Sea $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$.

(b) Defina $P_A = N$ y $S_A = \phi(N)$.

La función de cifrado Enc_{P_A} es definida de la siguiente forma. Dado un mensaje $m \in \{0, \ldots, N-1\}$, se genera al azar un número $r \in \{1, \ldots, N-1\}$ tal que $MCD(r, N) = 1$, y se construye

$$Enc_{P_A}(m) \quad = \quad ((N+1)^m \cdot r^N) \mod N^2$$

La función de descifrado Dec_{S_A} es definida de la siguiente forma. Sea $B \in \{0, \ldots, N-1\}$ el inverso de $\phi(N)$ en módulo N, vale decir, B satisface la condición

$$\phi(N) \cdot B \equiv 1 \mod N$$

Entonces dado un texto cifrado $c \in \{0, \ldots, N^2 - 1\}$, se define

$$Dec_{S_A}(c) \quad = \quad \left[\text{Div}(c^{\phi(N)} \mod N^2, N) \cdot B\right] \mod N$$

Responda las siguientes preguntas, en las cuales va a implementar el esquema criptográfico y va a demostrar que es correcto.

(a) Implemente el esquema criptográfico definido en esta pregunta completando el Jupyter notebook `pregunta1_a.ipynb`. Para que su pregunta sea considerada correcta, su notebook deberá correr de principio a fin habiendo completado los métodos marcadas con `##### POR COMPLETAR`. Las entradas y salidas de estos métodos no pueden ser modificadas, pero sí puede agregar métodos adicionales si los considera necesarios. Se evaluará con un programa externo la implementación de sus clases `Receiver` y `Sender`.

(b) Demuestre que $MCD(N, \phi(N)) = 1$. Nótese que de esto se deduce la existencia del número B, que es el inverso de $\phi(N)$ en módulo N.

(c) Dado $m \in \{0, \ldots, N-1\}$, demuestre que:

$$Dec_{S_A}(Enc_{P_A}(m)) \quad = \quad m$$

Solución.

(a) La solución de esta pregunta está en el Jupyter notebook `sol_p1_a.ipynb`.

(b) Sean P y Q dos números primos distintos tales que $P \geq 3$, $Q \geq 3$ y $\#\text{Bit}(P) = \#\text{Bit}(Q)$, y defina $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$. Con el fin de obtener una contradicción, suponga que $MCD(N, \phi(N)) > 1$.

Sin perdida de generalidad suponga que $P > Q$. Entonces se tiene que P no divide a $Q-1$, y por lo tanto no puede dividir a $\phi(N) = (P-1) \cdot (Q-1)$. Dado que $MCD(N, \phi(N)) > 1$, se debe tener entonces que Q divide a $P-1$. Como $P \geq 3$, se tiene que $P-1$ es un número par, vale decir, $P - 1 = 2 \cdot R$. Como Q es un número primo mayor o igual a 3 y Q divide a $2 \cdot R$, se debe tener que Q divide a R. De esto se deduce que $\#\text{Bit}(Q) \leq \#\text{Bit}(R)$. Pero $\#\text{Bit}(R) = \#\text{Bit}(P-1) - 1$, puesto que $P - 1 = 2 \cdot R$, de lo cual se concluye que $\#\text{Bit}(Q) \leq \#\text{Bit}(R) = \#\text{Bit}(P-1) - 1 \leq \#\text{Bit}(P) - 1 < \#\text{Bit}(P)$. De esto se obtiene una contradicción con el supuesto inicial de que $\#\text{Bit}(P) = \#\text{Bit}(Q)$.

Observe que es necesario suponer la condición $\#\text{Bit}(P) = \#\text{Bit}(Q)$ para obtener la propiedad $MCD(N, \phi(N)) = 1$. Por ejemplo, si $P = 11$ y $Q = 5$, entonces se tiene que $N = 55$, $\phi(N) = 40$ y $MCD(55, 40) = 5$. Pero en este caso se tiene que $\#\text{Bit}(P) \neq \#\text{Bit}(Q)$ puesto que $\#\text{Bit}(P) = 4$ y $\#\text{Bit}(Q) = 3$.

(c) Sea $m \in \{0, \ldots, N-1\}$, $r \in \{1, \ldots, N-1\}$ tal que $MCD(r, N) = 1$, y

$$c \quad = \quad ((N+1)^m \cdot r^N) \mod N^2.$$

Para demostrar que el protocolo es correcto, tenemos que demostrar que

$$m \quad = \quad \left[\text{Div}(c^{\phi(N)} \mod N^2,\, N) \cdot B\right] \mod N$$

Para esto, primero consideramos la expresión $c^{\phi(N)} \bmod N^2$. Dada la definición de c, tenemos que

$$\begin{aligned} c^{\phi(N)} \mod N^2 &= \left(((N+1)^m \cdot r^N) \mod N^2\right)^{\phi(N)} \mod N^2 \\ &= \left((N+1)^m \cdot r^N\right)^{\phi(N)} \mod N^2 \\ &= \left((N+1)^{m \cdot \phi(N)} \cdot r^{N \cdot \phi(N)}\right) \mod N^2 \\ &= \left((N+1)^{m \cdot \phi(N)} \cdot (r^{N \cdot \phi(N)} \mod N^2)\right) \mod N^2 \end{aligned} \tag{1}$$

Dado que $MCD(r, N) = 1$, se tiene que $MCD(r, N^2) = 1$. Como vimos en clases, de esto se concluye que $r^{\phi(N^2)} \bmod N^2 = 1$. Pero $N = P \cdot Q$ donde P y Q son dos primos distintos, por lo que $\phi(N^2) = N \cdot \phi(N)$, y se deduce que

$$r^{N \cdot \phi(N)} \mod N^2 \quad = \quad 1 \tag{2}$$

Por otro lado, por el teorema del binomio tenemos que

$$\begin{aligned}(N+1)^{m\cdot\phi(N)} &= \sum_{i=0}^{m\cdot\phi(N)} \binom{m\cdot\phi(N)}{i} N^i \\ &= 1 + m\cdot\phi(N)\cdot N + \alpha\cdot N^2,\end{aligned}$$

donde α es un número natural. Tenemos entonces que

$$(N+1)^{m\cdot\phi(N)} \mod N^2 = (1 + m\cdot\phi(N)\cdot N) \mod N^2.$$

Pero además sabemos que

$$1 + m\cdot\phi(N)\cdot N = \beta\cdot N^2 + (1 + m\cdot\phi(N)\cdot N) \mod N^2,$$

donde β es también un número natural. Concluimos entonces que

$$\begin{aligned}(N+1)^{m\cdot\phi(N)} \mod N^2 &= (1 + m\cdot\phi(N)\cdot N) \mod N^2 \\ &= 1 + m\cdot\phi(N)\cdot N - \beta\cdot N^2. \end{aligned} \tag{3}$$

Combinando (1), (2) y (3), obtenemos que

$$\begin{aligned}c^{\phi(N)} \mod N^2 &= \big((N+1)^{m\cdot\phi(N)} \cdot (r^{N\cdot\phi(N)} \mod N^2)\big) \mod N^2 \\ &= (N+1)^{m\cdot\phi(N)} \mod N^2 \\ &= 1 + m\cdot\phi(N)\cdot N - \beta\cdot N^2.\end{aligned}$$

Finalmente, de esto concluimos que el protocolo es correcto puesto que

$$\begin{aligned}\big[\mathrm{Div}(c^{\phi(N)} \mod N^2, N)\cdot B\big] \mod N &= \big[\mathrm{Div}(1 + m\cdot\phi(N)\cdot N - \beta\cdot N^2, N)\cdot B\big] \mod N \\ &= \Big[\Big\lfloor \frac{1 + m\cdot\phi(N)\cdot N - \beta\cdot N^2 - 1}{N} \Big\rfloor \cdot B\Big] \mod N \\ &= \big[(m\cdot\phi(N) - \beta\cdot N)\cdot B\big] \mod N \\ &= \big[m\cdot\phi(N)\cdot B\big] \mod N \\ &= m \mod N \\ &= m\end{aligned}$$

Nótese que para obtener las dos últimas igualdades consideramos que $\phi(N)\cdot B \equiv 1 \mod N$ y $m \in \{0, \ldots, N-1\}$.