Teoría de números y criptografía

Joshua Chicoj

Universidad del Valle de Guatemala

2023

Agenda

1. Criptografía
2. Cifrado simétrico
3. Cifrado asimétrico
4. Diffie-Hellman
5. El Gamal
6. RSA

Agenda

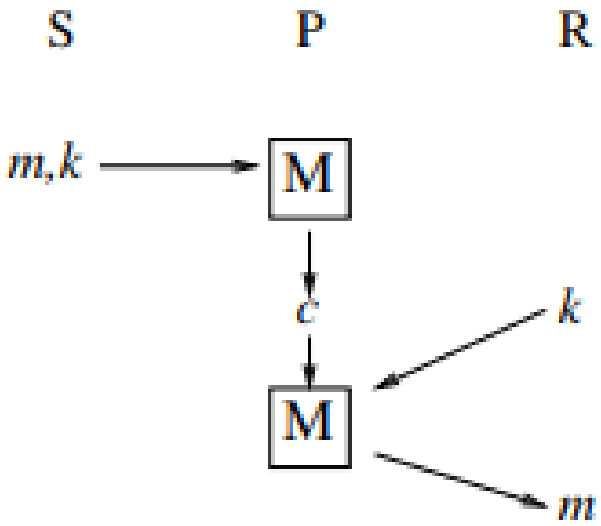
Criptografía

Proveniente del griego *cryptos* que significa "secreto, oculto". La criptografía es el arte de transofmar mensajes de tal forma que solo el destinatario correcto pueda entenderlo. Al proceso de transformar el mensaje se le conoce como encriptar, el mensaje oculto se llama criptograma y el proceso para revelar el mensaje se conoce como desencriptar.

Agenda

Cifrado simétrico

Sean S, R quienes envían y reciben un mensaje respectivamente. El cifrado simétrico consiste en enviar un mensaje m encriptándolo mediante una función $M : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ donde $\mathcal{K}, \mathcal{M}, \mathcal{C}$ representan el conjunto de posibles claves para encriptar, el conjunto de los posibles mensajes y el conjunto de los posibles mensajes cifrados respectivamente.



Cifrado simétrico

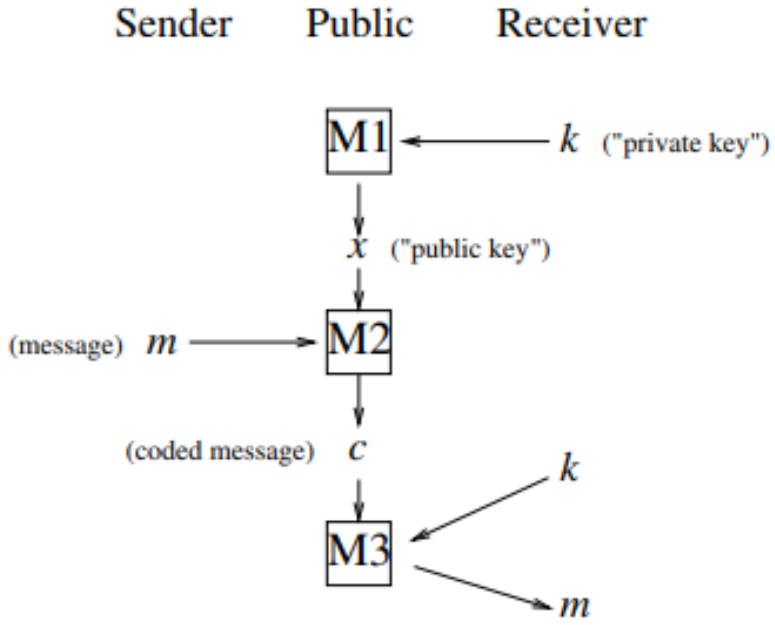
Algunos ejemplos de cifrado simétrico

- **Sustitución simple**: consiste en la sustitución de caracteres por otros de un mismo alfabeto. Su principal vulnerabilidad es el análisis de frecuencias
- **Cifrado polialfabético**: consiste en la sustitución de caracteres por otros de distintos alfabetos. El cambio de alfabeto se realiza de forma aleatoria y es señalado con una letra minúscula, el alfabeto a cambiar es señalado en el siguiente caracter. Su principal vulnerabilidad son los fragmentos repetidos
- **Multiplicación** mód p: el mensaje se encripta mediante $c := k \cdot m$ mód p. En el caso que un inceptor conozca m, c puede encontrar $k = m^{-1} \cdot c$ mód p

Agenda

Criptografía de llave pública

En este caso, "público"quiere decir que la llave pública x y el mensaje encriptado c se transmiten en un canal visible para todos y, por lo tanto, inseguro. Por ello se hace uso de una función $M_2 : \mathcal{M} \to \mathcal{C}$ la cual es fácil de calcular, pero difícil de invertir sin conocer la llave privada k



Criptografía de llave pública

Este tipo de cifrado se basa en las siguientes afirmaciones. Se considera más sencillo:

1. Verificar una factorización prima que factorizar un número
2. Calcular potencias $\mod n$ que calcular logaritmos $\mod n$
3. Calcular potencias $\mod n$ que calcular raíces $\mod n$

Sobre estas afirmaciones se basan el intercambio de llaves públicas Diffie-Hellman y los sistemas de encriptación El Gamal y RSA

Agenda

Discrete Logarithm Problem

Definición

Sea p un primo y $a \in \mathbb{Z} \ni (a, p) = 1$. Si $s \equiv a^m \mod p$ para algún m, entonces m es el **logaritmo discreto** de $s \mod p$ de base a

Si $a = g$ una raíz primitiva $\mod p$, entonces cualquier s coprimo a p puede ser escrito como g^m. El problema del logaritmo discreto consiste en calcular $m = \log_g a$

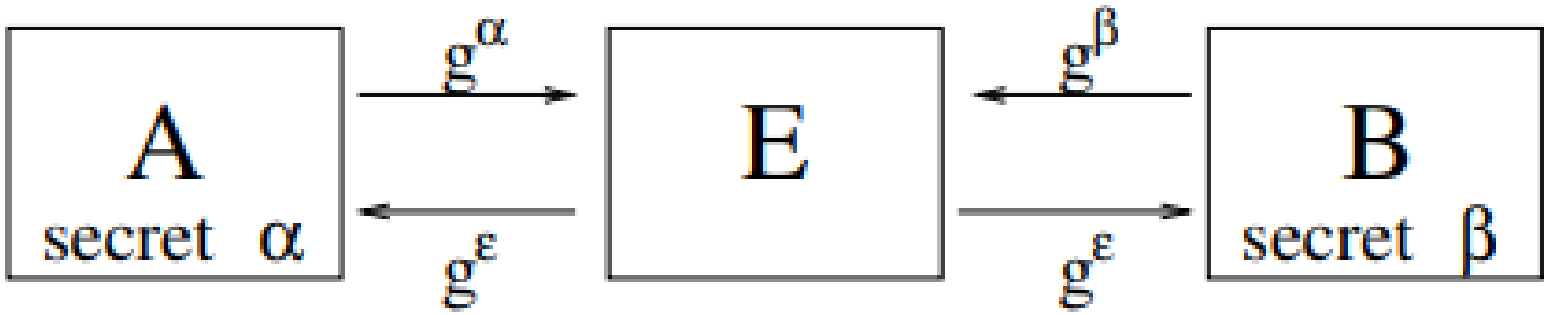
Diffie-Hellman

Es un algoritmo para la generación de llaves públicas entre dos entes A, B los cuales acuerdan utilizar p, un número primo, y $g \in \mathbb{Z}/p\mathbb{Z}$ una raíz primitiva mód p. A, B escogen aleatoriamente $\alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z}$ para luego enviarse g^α, g^β. Por lo tanto, el secreto compartido sería

$$\left.\begin{array}{l} \textbf{A computes } (g^\beta)^\alpha = g^{\alpha\beta} \\ \textbf{B computes } (g^\alpha)^\beta = g^{\alpha\beta} \end{array}\right\} =: s.$$

Si existiera E, un tercero intentando conocer el secreto, puesto que p, g, g^α, g^β son conocidos, debería calcular $\log g^\alpha$ o $\log g^\beta$ para conocer $g^{\alpha\beta}$. Esto implica resolver el DLP

El hombre en medio



Agenda

El Gamal

El criptosistema El Gamal involucra 4 pasos

1. Acordar un número primo p y una raíz primitiva $g \in \mathbb{Z}/p\mathbb{Z}$
2. El receptor escoge una llave privada $\rho \in Z \cap [1, p-2]$ y envía la llave pública $r = g^{\rho}$ al emmisor
3. El emisor escoge una llave temporal $\sigma \in \mathbb{Z} \cap [1, p-2]$ y un mensaje $m \in Z \cap [1, p-2]$. Luego envía al receptor el cifrado $(c_1, c_2) := (g^{\sigma}, mr^{\sigma})$ y se descarta σ
4. El receptor desencripta el mensaje calculando

$$c_1^{-\rho} \cdot c_2 \equiv g^{-\sigma\rho} \cdot mg^{\sigma\rho} \equiv m \mod p$$

El Gamal

- Alice desea enviarle un mensaje a Bob, por lo que acuerdan usar acuerdan usar $(p, g) = (1373, 2)$. Bob escoge la clave privada $\rho = 716$ y envía la clave pública $r = 2^{716} \equiv 469 \mod 1373$. Alice escoge la clave temporal $\sigma = 877$ y el mensaje $m = 583$. ¿Cuál es el mensaje cifrado que envía Alice a Bob?
- Bob quiere responder el mensaje de Alice, por lo que ella escoge la llave privada $\rho = 299$ y publica r_a. Bob utiliza la llave pública r_a publicada por Alice y envía el mensaje cifrado $(c_1, c_2) = (661, 1325)$. ¿Cuál es el mensaje desencriptado?

Agenda

RSA

El criptosistema RSA involucra los siguientes pasos

1. El receptor escoge 2 primos (suelen ser de al menos 200 dígitos) p, q y genera $n = pq$
2. El receptor escoge un exponente $k \ni (k, \phi(n)) = (k, (p-1)(q-1)) = 1$
3. El receptor calcula el inverso $e \in \mathbb{Z}/\phi(n)\mathbb{Z}$ de k
4. El receptor hace pública la clave (n, k)
5. El emisor genera el mensaje encriptado $c = m^k \mod n$ y lo envía al receptor
6. El receptor desencripta el mensaje calculando $c^e = m^{ke} \equiv m \mod n$

RSA

- Alice desea decirle a Bob que se detenga porque está a punto de caer a un precipicio, por lo que hace pública la clave $(n, k) = (2537, 13)$. ¿Cómo quedaría la palabra STOP encriptada mediante RSA?
- Bob no logró decencriptar el mensaje a tiempo, por lo que cayó al precipicio y le envía a Alice el mensaje encriptado 0981 0461. ¿Qué dice el mensaje?

Referencias

- McGraw Hill Education. (s. f.). Number Theory and Cryptography [Diapositivas]. https://www.cs.wm.edu/. https://www.cs.wm.edu/ tadavis/cs243/ch04s.pdf
- Kerr, M. K. (s. f.). Lecture notes Number Theory and Cryptography.
- Coutinho, S. C. (1999). The Mathematics of Ciphers: Number Theory and RSA Cryptography. Choice Reviews Online, 37(01), 37-0363. https://doi.org/10.5860/choice.37-0363