Sistemas criptográficos clásicos

Matemática Discreta 2
CENUR Noreste - Sede Tacuarembó

17 de junio de 2026

Cifrado "César" (Julio César, Roma 100-44 A.C.)

Vamos a utilizar una correspondencia entre letras y números:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ejemplo

Cifrar la letra Y con César, usando la clave privada $k = 4$.

1. a Y se le asocia su número de la tabla: $x = 25$.
2. se cifra el número $x = 25$, con la clave $k = 4$, mediante:

$$25 + 4 \pmod{28} \equiv 29 \pmod{28} \equiv 1 \pmod{28}.$$

3. el número cifrado es $y = 1$, que corresponde a la letra B.

En general, el cifrado César de un número x, es:

$$y \equiv x + k \pmod{n};$$

k es la clave privada, y n la cantidad de símbolos del alfabeto.

Descifrado César

Queremos obtener x a partir del valor cifrado y. Despejando:

$$y \equiv x + k \pmod{n} \Leftrightarrow x \equiv y - k \pmod{n}.$$

Se debe conocer la clave privada k con la que fue cifrado x.

Ejemplo

Descifrar la letra B, con la clave privada $k = 4$:

1. a B se le asocia su número de la tabla: y=1.
2. se descifra y como:

$$y - k \pmod{n} \equiv 1 - 4 \pmod{28} \equiv 25 \pmod{28}.$$

3. el número descifrado 25 corresponde a la letra Y.

Sistema afín

- César es muy sencillo de romper: se descifra el mensaje con cada uno de los 28 valores posibles de k, hasta obtener una frase con sentido.
- El sistema afín es una generalización del César, que agrega mayor seguridad. El **cifrado** afín de un número x es:

$$y \equiv ax + k \pmod{n}.$$

- La clave privada es el par (a, k). El **descifrado** afín es:

$$y \equiv ax + k \pmod{n} \Leftrightarrow y - k \equiv ax \pmod{n} \Leftrightarrow$$

$$\Leftrightarrow x \equiv b\,(y - k) \pmod{n};$$

donde b es el inverso de a módulo n: $ba \equiv 1 \pmod{n}$. Para que dicho inverso exista, pedimos $\gcd(a, n) = 1$.

Sistema Vigenère

- Otra generalización del sistema César, donde ahora la clave privada es una palabra (vs. una letra).

Ejemplo

Cifrar "YA_ES_HORA", utilizando la **palabra** clave "SOL".

Y	A	_	E	S	_	H	O	R	A
S	O	L	S	O	L	S	O	L	S

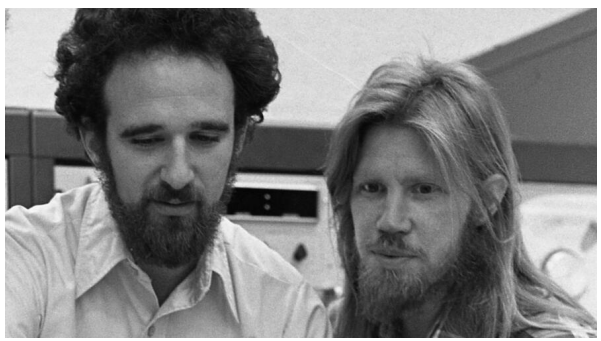
Ciframos como en César, pero con clave dependiente de la posición: Y con la clave S, A con O, _ con L, E con S, ...

Descifrado: en lugar de sumar la clave, la restamos (módulo 28).

- La cantidad de palabras clave posibles crece exponencialmente con el tamaño del texto, lo que hace al método más seguro.

Intercambio de la clave privada

- Los sistemas anteriores requieren que el remitente y destinatario utilicen la misma clave privada (para cifrar y descifrar).
- En los tiempos de César la clave se intercambiaba en un encuentro personal.
- En la actualidad necesitamos métodos de intercambio de clave a distancia, y que sean suficientemente seguros.
- Uno de los más conocidos es el método de Diffie-Hellman, propuesto en 1976 por investigadores de Stanford.



Diffie-Hellman (1976)

Ana y Brian quieren intercambiar una clave privada k. Se ponen de acuerdo públicamente en elegir (p, g); p primo, $1 < g < p$.

1. **Ana** selecciona un natural n aleatorio (privado), calcula g^n (mód p), y lo envía a Brian (públicamente).
2. **Brian** selecciona un natural m aleatorio (privado), calcula g^m (mód p), y lo envía a Ana (públicamente).

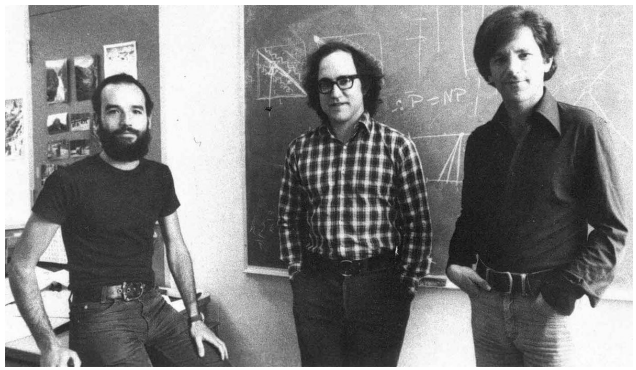
La clave privada es: $k \equiv g^{n \times m} \pmod{p}$. Ambos la pueden calcular fácilmente, tomando potencias módulo p:

$$k \equiv g^{n \times m} \pmod{p} \equiv (g^n)^m \pmod{p} \equiv (g^m)^n \pmod{p}.$$

¿Un intruso podría calcular k? Sí, pero primero debe calcular n o m. Equivale a calcular un **logaritmo discreto** (inverso de la exponenciación), que es considerado un problema difícil.

Sistemas de clave pública - RSA (1977)

- Uno de los más conocidos es el método RSA, propuesto en 1977 por **R**ivest, **S**hamir y **A**dleman.



- Basa su seguridad en el hecho de que calcular los factores primos de un número es un problema difícil en general.
- RSA-129 (129 dígitos decimales):

$$n = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597\ldots$$
$$\ldots 123563958705058989075147599290026879543541.$$

- 100 dólares de recompensa a quien halle p y q primos, tal que: $n = p \times q$. Propuesto en 1977, factorizado en 1994.

RSA

Ana desea recibir mensajes cifrados. Genera su clave pública:

1. selecciona dos primos p y q, y calcula su producto $n = p \times q$.
2. selecciona e, tal que: $1 < e < \varphi(n) = (p-1)(q-1)$.
3. publica el par (n, e), que es su clave pública personal.

Brian quiere enviar un mensaje a Ana. Para esto:

1. busca la clave pública de Ana: (n, e).
2. **cifra** x mediante: $y = x^e \pmod{n}$, y lo envía a Ana (público).

Ana recibe el mensaje y de Brian. Para **descifrarlo**:

1. calcula d tal que: $d \times e \equiv 1 \pmod{\varphi(n)}$. $(\gcd(e, \varphi(n)) = 1)$.
2. el mensaje descifrado es: $x \equiv y^d \pmod{n}$.

Calcular d requiere calcular $\varphi(n)$. Esto es tan difícil como factorizar n en primos (obtener p y q).

RSA - Ejemplo

Ana genera su clave pública:

1. selecciona dos primos $p = 3$ y $q = 7$, y calcula $n = 3 \times 7 = 21$.
2. $\varphi(n) = (p-1)(q-1) = 2 \times 6 = 12$.
3. selecciona $e = 5$: $1 < e < \varphi(n) = 12$, coprimo con $\varphi(n)$.
4. publica su clave pública personal: $(n, e) = (21, 5)$.

Brian quiere enviar el mensaje $x = 10$ a Ana. Para esto:

1. busca la clave pública de Ana: $(n, e) = (21, 5)$.
2. **cifra** $x = 10$ con RSA, y lo envía a Ana:

$$y = x^e \pmod{n} = 10^5 \pmod{21} \equiv 19 \pmod{21}.$$

Ana recibe el mensaje y de Brian. Para **descifrarlo**:

1. calcula d tal que: $de \equiv 1 \pmod{\varphi(n)}$. Esto es:

$$5 \times d \equiv 1 \pmod{12} \Leftrightarrow d \equiv 5 \pmod{12}.$$

2. el mensaje descifrado es:

$$x \equiv y^d \pmod{n} \equiv 19^5 \pmod{21} \equiv 10 \pmod{21}.$$

RSA - ¿Funciona?

- La función de **cifrado** es: $y = C(x) := x^e \pmod{n}$.
- La función de **descifrado** es:

$$D(y) := y^d \pmod{n}, \quad d \times e \equiv 1 \pmod{\varphi(n)}.$$

- ¿La función de descifrado siempre recupera el mensaje?:

$$¿D(C(x)) \equiv x \pmod{n},\ \forall\ x \in \mathbb{Z}? \Leftrightarrow x^{ed} \equiv x \pmod{n}.$$

- Es sencillo probar que sí. La prueba utiliza los teoremas de Fermat y Euler para calcular la potencia. Considera tres casos:
  1. p y q dividen a x: $x \equiv 0 \pmod{p}$, $x \equiv 0 \pmod{q}$ (trivial).
  2. sólo p divide a x: $x \equiv 0 \pmod{p}$, y $\gcd(x, q) = 1$ (Fermat).
  3. ni p ni q dividen a x: $\gcd(x, n) = 1$ (Euler).

RSA - Ataque de Fermat

- Si p y q son cercanos entre sí, es sencillo factorizar $n = p \times q$.
- Supongamos que conseguimos enteros t y s, con $t > s$, y:

$$n + s^2 = t^2.$$

Despejando:

$$n = t^2 - s^2 = (t - s)(t + s).$$

- Como sabemos que $n = p \times q$, y la factorización en primos es única, necesariamente: $p = t - s$, $q = t + s$ (o al revés).
- Fermat: calcular $n + s^2$, desde $s = 1$ y hasta obtener $s \geq 1$, tal que: $n + s^2 = t^2$. Esto factoriza n, por lo explicado antes.
- Este método de factorización funciona siempre (es sencillo ver que para). Pero puede requerir probar muchos valores de s.
- Sin embargo, si $p \simeq q$, entonces $t - s \simeq t + s$, y s es pequeño.