2019-10-16

Continuación encryptación

$E(x) = 3x + 5$

A T T A C K

0 19 19 0 2 10

E(x)

5 10 10 5 11 9

...

Entonces:

$D(x) = (x-5) \cdot 9$

$= 9x - 9 \cdot 5$

$= 9x - 45$

$\equiv_{26} 9x + 7$

F K K F L J

5 10 10 5 11 9

D(x)

0 19 19 0 2 10

A T T A C K

n - grama

- telegrama de mexico.

Definimos la función de desencriptado $D(x)$ como:

$$D(x) = (x - 5) \cdot 3^{-1}$$

Buscamos 3^{-1} en $\mathbb{Z}_{26}$:

Procedimiento:

$a = 3 \quad b = 26$

$\text{mcd}(26, 3)$

$26 = 3 \cdot 8 + 2$

$\text{mcd}(3, 2)$

$3 = 2 \cdot 1 + 1$

$\text{mcd}(2, 1)$

$2 = 1 \cdot 2 + 0$

Bézout:

$3 - 2 \cdot 1 = 1$

$3 - (26 - 3 \cdot 8) \cdot 1 = 1$

$3 - 26 - 8 \cdot 3 = 1$

$-26 + 9 \cdot 3 = 1$

$\mathbb{Z}_{26}$

$1 \equiv_{26} 9 \cdot 3$

$\therefore 3^{-1} \equiv_{26} 9$

...

Resumen: Estos son cifrados tipo césar (shift & ponderado) son sistemas criptográficos de sustitución; un caracter x siempre será sustituido por un mismo caracter y.
Esto representa la principal debilidad de dicho sistema, pues es altamente vulnerable a un ataque por análisis de frecuencia.

En el ataque por fuerza bruta:

C. Shift $E(x) = x + d$
Diccionario 26! y por la "d" $26 \cdot 26!$

C. Ponderado $E(x) = k\,x + d$
Diccionario 26! y contando k solo puede tener
$k: 26 - 1 - 1 - \text{floor}\left(\frac{25}{2}\right) = 12$ en total $12 \cdot 26 \cdot 26!$

Exponenciación modular: es hacer cálculo con números grandes usando aritmética modular; Un algoritmo que permite evaluar de forma eficiente, cantidades como:

$a^b \bmod(n)$

Ej: Calcule $7^{100} \bmod(91)$
Primero escribimos el exponente en binario

$100_2 = 1\ 1\ 0\ 0\ 1\ 0\ 0$
$2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$

$100 - 2^6 = 36$
$36 - 2^5 = 4$
$4 - 2^2 = 0$

$100 = 2^6 + 2^5 + 2^2$

...

... Queremos calcular 2^{100}:

$$2^{2^6 + 2^5 + 2^4} = 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^2}$$

	Bits	a^{2^n}	$a^{2^{n+1}} \bmod(n)$
lsb	0	2	4
	0	4	16
* →	1	16	$256 \equiv_{91} 74$
	0	74	$5476 \equiv_{91} 16$
	0	16	$256 \equiv_{91} 74$
* →	1	74	$5476 \equiv_{91} 16$
* → msb	1	16	$256 \equiv_{91} 74$

... me voy a quedar sólo con los unos

finalmente, $2^{100} = 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^2}$ $\quad \mathbb{Z}_{91}$

$\equiv_{91} 16 \cdot 74 \cdot 16$

$\equiv_{91} 16^2 \cdot 74 \equiv_{91} 74 \cdot 74$

$\equiv_{91} 16$