Ataques estadísticos

© Santiago Hernández Ramos

Otros métodos de ataque

Time memory trade-off attacks: El atacante construye una tabla con texto cifrado a partir de texto plano enviado frecuentemente utilizando un número muy elevado de claves. Cuando el atacante intercepta un texto cifrado para el que conoce o supone el texto plano, comprueba en la tabla si se encuentra la clave.

Primitive-specific attacks: *Differencial and linear cryptoanalysis, Birthday attacks, Statistical attacks...*

Side-channel attacks: Estos ataques no se realizan directamente sobre el criptosistema sino contra su implementación. Algunos de los más interesantes: *Timing attacks, Power analysis, Fault analysis...*

© Santiago Hernández Ramos

Ataques estadísticos | Análisis de frecuencia

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Porcentaje	12,53%	1,42%	4,68%	5,86%	13,68%	0,69%	1,01%	0,70%	6,25%	0,44%	0,02%	4,97%	3,15%	6,71%
Letra	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Porcentaje	0,31%	8,68%	2,51%	0,88%	6,87%	7,98%	4,63%	3,93%	0,90%	0,01%	0,22%	0,90%	0,52%	

```
DE :  2.57      AD :  1.43      TA :  1.09
ES :  2.31      AR :  1.43      TE :  1.00
EN :  2.27      RE :  1.42      OR :  0.98
EL :  2.01      AL :  1.33      DO :  0.98
LA :  1.80      AN :  1.24      IO :  0.98
OS :  1.79      NT :  1.22      AC :  0.96
ON :  1.61      UE :  1.21      ST :  0.95
AS :  1.56      CI :  1.15      NA :  0.92
ER :  1.52      CO :  1.13      RO :  0.85
RA :  1.47      SE :  1.11      UN :  0.84
```

```
DEL :  0.75     EST :  0.48     PAR :  0.32
QUE :  0.74     LOS :  0.47     DES :  0.31
ENT :  0.67     ODE :  0.47     ESE :  0.30
ION :  0.56     ADO :  0.45     IEN :  0.30
ELA :  0.55     RES :  0.40     ALA :  0.29
CON :  0.54     STA :  0.38     POR :  0.29
SDE :  0.52     ACI :  0.36     ONE :  0.29
ADE :  0.51     LAS :  0.35     NDE :  0.29
CIO :  0.50     ARA :  0.34     TRA :  0.28
NTE :  0.49     ENE :  0.32     NES :  0.27
```

```
CION :  0.42    MENT :  0.16    NCIA :  0.14
DELA :  0.33    IONE :  0.16    AQUE :  0.14
ACIO :  0.27    ODEL :  0.16    SQUE :  0.14
ENTE :  0.25    ONDE :  0.16    ENCI :  0.13
ESTA :  0.22    OQUE :  0.15    ENLA :  0.13
ESDE :  0.22    IDAD :  0.15    ENTR :  0.13
PARA :  0.19    ELOS :  0.15    IENT :  0.12
ONES :  0.17    ADEL :  0.15    ASDE :  0.12
SDEL :  0.17    ANTE :  0.15    ENEL :  0.12
OSDE :  0.17    ENTO :  0.14    DELO :  0.12
```

© Santiago Hernández Ramos