cifrario di Vigenère

- è un cifrario polialfabetico
- m un intero positivo - sarà la lunghezza della chiave
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
- se $k = (k_1, k_2, \dots, k_m)$ si ha
 - $e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
 - $d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$
- tutto modulo 26
- esempio: sia $m = 5$ e $k = (5, 8, 14, 17, 4)$
- se $x = (4, 0, 17, 17, 8)$, allora $e_k(x) = (9, 8, 5, 8, 12)$
- la crittoanalisi è molto più difficile!

cifrario di Hill

- è un cifrario polialfabetico
- m un intero positivo: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ pensati come vettori colonna
- $\mathcal{K} = \{\text{matrici } m \times m \text{ a coefficienti in } \mathbb{Z}_{26} \text{ invertibili in } \mathbb{Z}_{26}\}$
- $K \in \mathcal{K}$ è una matrice $m \times m$, $x \in \mathcal{P}$ è una m -pla; la cifratura è il prodotto righe per colonne
 - $e_K(x) = Kx$
 - $d_K(y) = K^{-1}y$
- tutto modulo 26
- la funzioni di cifratura e decifratura sono trasformazioni lineari
- quali sono le matrici invertibili in $\mathbb{Z}_{26}$?

- una matrice A a coefficienti reali è invertibile $\iff \det(A) \neq 0$
- una matrice A a coefficienti in $\mathbb{Z}_n$ è invertibile $\iff \det(A)$ è invertibile in $\mathbb{Z}_n \iff (\det(A), n) = 1$
- esempio: $n = 26$, $K = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}$, $\det(K) = 53 = 1$
- $K^{-1} = \begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 23 \\ 18 & 11 \end{pmatrix}$
- $e_K \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 28 \\ 30 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$
- $d_K \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 & 23 \\ 18 & 11 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 106 \\ 80 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$

cifrario lineare affine

- generalizza il cifrario di Hill
- m un intero positivo: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
- $\mathcal{K} = \{(A, b), A \text{ matrice invertibile}, b \in (\mathbb{Z}_{26})^m\}$
- se $k = (A, b)$, si ha
 - $e_k(x) = Ax + b$
 - $d_k(y) = A^{-1}(y - b)$
- tutto modulo 26
- la funzioni di cifratura e decifratura sono trasformazioni affini
- tutti i cifrari visti fino a ora sono di questo tipo!

crittoanalisi: principio di Kerckhoffs

L'attaccante, Eve, può conoscere il crittosistema usato da Alice e Bob.

Non conosce la chiave.

Vantaggi:

- è più facile tenere segreta la chiave
 - se la sicurezza si basa sulla chiave, e la chiave viene scoperta, basta cambiare chiave
 - si può usare lo stesso crittosistema per far comunicare diverse coppie di persone
-
- oggi il principio di Kerckhoffs viene inteso in maniera più forte: l'algoritmo deve essere pubblico
 - un sistema che viene molto studiato (e attaccato) è più sicuro
 - meglio che le debolezze, se ci sono, vengano scoperte e rese pubbliche
 - se l'algoritmo è pubblico, non c'è rischio di reverse engineering
 - si possono stabilire standard

crittoanalisi: tipi di attacco

Ciphertext only attack: L'attaccante conosce una stringa y di testo cifrato. Cerca di risalire al testo in chiaro o alla chiave.

Known plaintext attack: L'attaccante conosce una stringa x di testo in chiaro e il corrispondente testo cifrato y . Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen plaintext attack: L'attaccante ha la possibilità di scegliere un testo in chiaro x e di costruire il corrispondente testo cifrato. Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen ciphertext attack: L'attaccante ha la possibilità di scegliere un testo cifrato y e di ottenere il corrispondente testo in chiaro x . Cerca di risalire alla chiave.

crittoanalisi di un cifrario affine

XKLJS UJNXD YBUJT YOBLR GXUJD XKJWL TYXSX
ALYQX LAAJY RGXWX UXNNX KBRGJ LKLVX YQXRG
XRBNX KLUJN XDYLJ SJYQX KYBUX SOBL

la sostituzione è del tipo $e_{a,b}(x) = ax + b = y$:
basta trovare due coppie (x_1, y_1) e (x_2, y_2) tali che
 $ax_1 + b = y_1$ e $ax_2 + b = y_2$ per determinare a, b .

analisi delle frequenze

frequenze dei caratteri % in italiano

A	B	C	D	E	F	G	H	I
10,41	0,95	4,28	3,82	12,62	0,75	2,01	1,10	11,62
J	K	L	M	N	O	P	Q	R
0	0	6,61	2,58	6,49	8,71	3,20	0,75	6,70
S	T	U	V	W	X	Y	Z	
6,04	6,06	3,04	1,51	0	0	0	0,93	

crittoanalisi di un cifrario affine

Sono 99 caratteri, così distribuiti

A	B	C	D	E	F	G	H	I
3	6	0	3	0	0	4	0	0
J	K	L	M	N	O	P	Q	R
10	6	10	0	5	2	0	3	5
S	T	U	V	W	X	Y	Z	
4	2	6	1	2	18	9	0	

Probabilmente $e \rightarrow X$
quindi $4a + b = 23$.

Proviamo $a \rightarrow J$
allora $a \cdot 0 + b = 9$.

La congruenza $4a \equiv 14 \pmod{26}$
ha due soluzioni: $a = 10$ (che non può essere)
e $a = -3 = 23$.
10 non va bene: $(10, 26) \neq 1$.

Proviamo la sostituzione $y = 23x + 9$. Si ha $23^{-1} = 17$,
quindi $x = 17(y - 9)$.

Decifrando, si ha

erix faqec vufao vhuig befac erani ovexe
ivpei ddavg benef eqqer ugbai riwev pegbe
guqer ifaqe cvi ax avper vufex hui

Proviamo $a \rightarrow L$
allora $a \cdot 0 + b = 11$.
e $4a + b = 23$.

La congruenza $4a \equiv 12 \pmod{26}$
ha le due soluzioni $a = 3$ e $a = 16$.
16 non va bene: $(16, 26) \neq 1$.

Proviamo la sostituzione $y = 3x + 11$. Si ha $3^{-1} = 9$,
quindi $x = 9(y - 11)$.

Decifrando, si ha

erail diseg nodiu nboac hedig eriva unele
fante affin cheve desse rochi arame ntech
ecose radis egnai linte rnode lboa