Quarta lezione

Tavola 18: Le chiavi del cifrario affine e gli invertibili quando *n* è primo
Tavola 19: Le chiavi del cifrario affine e gli invertibili quando *n* è prodotto di due primi distinti. (Facoltativa)
Tavola 25 (Facoltativa): somma di invertibili

ONE TIME PAD

E' possibile creare un cifrario perfetto, impossibile da decifrare senza conoscere la chiave
Si usa il sistema di Vigenère con una chiave

- lunga (almeno) quanto il messaggio da cifrare
- generata a caso, senza nessun significato **da usare una sola volta.**

E' impossibile da decifrare: il messaggio ABCDEF potrebbe significare

- domani (chiave UMPDQU)
- vivere (chiave CQEZMB)
- papera (chiave ....)
- ….

Il problema è che A e B si devono mettere preventivamente d'accordo scegliendo tante chiavi quanti messaggi si devono scambiare
Tavola 20: One Time Pad

CIFRATURA A BLOCCHI

L'operazione di cifratura a blocchi sfrutta il fatto che l'alfabeto in chiaro sia formato da numeri (tutti della stessa lunghezza).
Modifico la corrispondenza inizialmente proposta tra alfabeto e numeri, facendo in modo che i numeri utilizzati siano formati dallo stesso numero di cifre:

a	b	c	d	e	f	g	h	i	l
00	01	02	03	04	05	06	07	08	09

m	n	o	p	q	r	s	t	u	v	z
10	11	12	13	14	15	16	17	18	19	20

Ogni parola viene trasformata in una sequenza di coppie di numeri.
Comunque fissato un numero naturale n, raggruppo le cifre in blocchi ottenuti a partire da sinistra in modo da avere sempre numeri $< n$.
Ad esempio, per $n = 1000$, raggruppo 4 cifre alla volta (corrispondenti a due lettere dell'alfabeto):
Si osservi che dai blocchi così ottenuti è possibile ricostruire l'informazione iniziale in modo perfetto: basta suddividere in coppie il blocco (partendo da sinistra).

Ora posso cifrare i singoli blocchi: chi decifra ritroverà il blocco in chiaro, e procederà a suddividerlo per ritrovare le cifre iniziali.

Non è necessario rispettare la suddivisione in coppie nella formazione dei blocchi: ad esempio posso formare blocchi di lunghezza dispari.

Tavola 21 Cifratura a blocchi
Le potenze

Giocando con le operazioni in $\mathbf{Z}_n$, e' possibile cercare altre cifrature.
Cosa succede se, per cifrare, elevo ogni elemento ad una potenza fissata? Sto considerando l'applicazione: $\mathbf{Z}_n \to \mathbf{Z}_n$ definita da: $x \mapsto x^t$.
Sono trasformazioni accettabili come cifrature?

Provo ad elevare al quadrato **Modulo 10**:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\mathbf{x^2}$	**0**	**1**	**4**	**9**	**6**	**5**	**6**	**9**	**4**	**1**

L'elevamento al quadrato non è una trasformazione iniettiva e suriettiva.
C'è un esponente corretto da usare?

Tavola 22 Le potenze in $\mathbf{Z_5}$.
Tavola 23 Introduzione al Piccolo Teorema di Fermat

Mostriamo che, quando *n* è primo, gli esponenti che possiamo utilizzare sono solo un numero finito (limitato da *n*) (dunque, le chiavi di cifratura sono in numero limitato):

Piccolo teorema di Fermat: *Se p è un numero primo ed a non è divisibile per p, allora*

$$a^{p-1} = 1 \mod p.$$

Dimostrazione. L'elemento *a* è invertibile modulo p e quindi la moltiplicazione per *a* è iniettiva e manda 0 in 0.
L'insieme formato dagli elementi

$\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$

coincide quindi con $\{1, 2, \ldots, p-1\}$.
Quindi il prodotto degli elementi del primo insieme deve essere uguale al prodotto di quelli del secondo:

$$a^{p-1}\,(p-1)\,(p-2)\ldots\ldots 2 = (p-1)\,(p-2)\ldots\ldots 2$$

Poichè $(p-1)\,(p-2)\ldots\ldots 2$ è invertibile, ottengo la tesi. ◊

Tavola 24: continuazione della frase