II LEZIONE

La cifratura di messaggi ha un ruolo così importante che nel tempo si sono sviluppati macchinari per cifrare più velocemente.
Il primo esempio di macchina per cifrare è il cosiddetto disco cifrante di Leon Battista Alberti. Esso consiste di due dischi concentrici, di diametri differenti, che sono imperniati nel centro su di un perno, e possono così ruotare l'uno rispetto all'altro attorno ad esso: lungo le circonferenze dei due dischi sono incisi due alfabeti. Nella circonferenza interna c'è l'alfabeto in chiaro, in quella esterna l'alfabeto cifrante. Per criptare un messaggio con la cifratura per traslazione utilizzando come chiave k=5 basta collocare la lettera a del disco interno in corrispondenza della lettera F sul disco esterno. Fatta questa semplice operazione ad ogni lettera dell'alfabeto in chiaro resta associata una lettera dell'alfabeto cifrato e così senza dover più ruotare i dischi si può trascrivere il messaggio vedendo quale lettera del disco esterno corrisponde alla lettera del disco interno che dobbiamo scrivere.

Abbiamo visto che questo metodo, che opera semplicemente traslando, è facilmente attaccabile sia con l'analisi delle frequenze sia per tentativi, cioè provando tutte le sole 20 combinazioni possibili. È necessari quindi trovare un metodo di cifratura più efficace e sicuro.
Abbiamo visto che considerando le lettere come elementi di Z_{21} potevamo modellizzare la procedura di cifratura per traslazione nel modo seguente:
data la chiave $k \in K$, la funzione cifrante è:

$$C_k : Z_{21} \to Z_{21}$$
$$p \to p + k \mod 21,$$

mentre la funzione inversa, quella di decifratura, è:

$$D_k : Z_{21} \to Z_{21}$$
$$c \to c - k \mod 21.$$

La traslazione offre poche possibilità (solo 20) perché è un procedimento troppo semplice: tre lettere consecutive dell'alfabeto in chiaro (ad esempio a, b, c) vengono cifrate con tre le lettere consecutive dell'alfabeto cifrante (ad esempio D,E,F se la chiave è k=3). Bisognerebbe eliminare questa regolarità, questo schema con cui si susseguono le lettere. Per farlo è necessario "complicare" la funzione di cifratura C_k. *Discussione*

L'idea è quella di mescolare le lettere e di disporle in un ordine apparentemente casuale ma che almeno per noi e per il destinatario del nostro messaggio mantenga una logica ben precisa.

Dato che, ormai, stiamo lavorando nel nuovo insieme Z_{21} per capire meglio come procedere bisogna analizzare più in dettaglio le caratteristiche e le proprietà di questo insieme; trattiamo il caso generale Z_n delle classi di resto modulo n.
Proprio come in Z , vi si possono definire operazioni che ci consentono di trattare le classi si resto quasi come numeri interi. E' possibile definire somma, prodotto e creare tutta un'aritmetica che viene definita aritmetica modulare perché si lavora modulo n (nel senso delle congruenze).

DEF. Date $\overline{a}$ $\overline{b}$ due classi di resto modulo n si ha che:

- $\overline{a} + \overline{b} = \overline{a + b}$
- $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Per comodità di calcolo esprimeremo il risultato di queste operazioni sempre tramite il suo rappresentante cioè se, ad esempio, stiamo lavorando modulo 5 e dobbiamo calcolare la somma tra $\bar{3}$ e $\bar{4}$ faremo $\bar{3}+\bar{4}=\overline{7}=\bar{2}$ poiché $7 \equiv 2\ (5)$ e similmente per il prodotto.

Esercizi su somma e prodotto e potenze.

- Calcolare $\overline{19}+\bar{7}$ modulo 21
- Calcolare $\bar{4}\cdot\bar{7}$ modulo 21
- A che classe modulo 21 appartiene $5\cdot 9+12$

Osserviamo che la definizione di queste di queste operazioni è ben posta cioè è indipendente dal rappresentante della classe che si sceglie per operare.
Infatti:
$\overline{18}+\overline{21}=\overline{39}\ \ (4)$
e $\overline{39}=\bar{3}\ (4)$ perché $39=4\cdot 9+3$
ma $\overline{18}=\bar{2}$ (perché $18=4\cdot 4+2$) e $\overline{21}=\bar{1}$ perché $21=4\cdot 5+1$ allora
$\overline{18}+\overline{21}=\bar{2}+\bar{1}=\bar{3}=\overline{39}$
Lo stesso vale per il prodotto:
$\bar{5}\cdot\bar{4}=\overline{20}=\bar{2}\ \ (6)$
e $\overline{17}\cdot\overline{10}=\overline{170}=\bar{2}\ (6)$
perché $\overline{17}=\bar{5}\ (6)$ e $\overline{10}=\bar{4}\ (6)$

Per comodità di calcolo, come abbiamo specificato anche in fase di definizione, sceglieremo sempre come rappresentanti delle classi di resto modulo *n* i numeri $\bar{b}$ tali che $0 \le b \le n-1$.

Inoltre notiamo che entrambe le operazioni definite sono dotate di un elemento particolare, proprio come in Z dove esistono lo 0 che non modifica una somma (ad es. 12934+0=12934) e l'1 che non cambia un prodotto (ad es. $23458\cdot 1=23458$). In Z_n essi sono rispettivamente $\bar{0}$ e $\bar{1}$ infatti preso un altro qualsiasi elemento $\bar{a}\in Z_n$ vale che:
$\bar{a}+\bar{0}=\bar{a}$
$\bar{a}\cdot\bar{1}=\bar{a}$

Questo deriva dalla definizione delle operazioni somma e prodotto. *Si può discuterne*
Infatti:
$\bar{a}+\bar{0}=\overline{a+0}=\bar{a}$
$\bar{a}\cdot\bar{1}=\overline{a\cdot 1}=\bar{a}$

Non bisogna però pensare che tutto quello che vale per l'uguaglianza valga automaticamente anche per la congruenza cioè non tutte le operazioni con cui siamo soliti lavorare in Z restano valide in Z_n. Ad esempio la legge di cancellazione $a\cdot b=a\cdot c \Rightarrow b=c$ che vale in Z purché sia $a\neq 0$ non si trasporta alle congruenze ad esempio:
$3\cdot 5\equiv 3\cdot 8\equiv 6\ (9)$ ma non è vero che $5\equiv 8\ (9)$
Quindi purtroppo operando con le classi di resto in generale non è vero che se $\bar{a}\cdot\bar{b}=\bar{a}\cdot\bar{c}$ allora $\bar{b}=\bar{c}$ come mostra l'esempio.

A questo punto possiamo già avere un'idea di come perfezionare la funzione di cifratura C_k.

Possiamo definire un'applicazione C_k che non solo contenga una traslazione ma anche una moltiplicazione. Allora
la nostra chiave sarà una coppia di numeri $k = (a,b)$
e la funzione cifrante sarà $C_k : Z_{21} \to Z_{21}$

$$p \to a \cdot p + b \mod 21,$$

Questo sistema prende il nome di **cifrario affine**.
Il problema è ora capire se questa funzione va bene, cioè dobbiamo vedere se ad ogni lettera dell'alfabeto in chiaro corrisponde una diversa lettera dell'alfabeto cifrante (perché questo ci assicura che, così, è possibile decifrare in modo univoco il testo) . Ovvero dobbiamo verificare che la funzione C_k è biunivoca.

Ricordiamo che una funzione tra due insiemi A (dominio) e B (condominio) è biunivoca se è iniettiva e suriettiva.
È iniettiva se ad elementi distinti di A corrispondono elementi distinti di B.
È suriettiva se ogni elemento di B è immagine di un elemento di A.

Nel nostro caso, quindi, dobbiamo verificare che :

- prese due lettere distinte dell'alfabeto in chiaro queste vengano criptate con lettere diverse (iniettività)
- ad ogni lettera dell'alfabeto cifrante resta associata una lettera dell'alfabeto in chiaro (suriettività).

Iniziamo con il vedere in dettaglio due casi:
scegliamo $k = (3,4)$ e $k = (5,4)$; il che equivale a dire che operiamo sempre la stessa traslazione, 4, ma come agente mescolante usiamo due numeri diversi, una volta 3 e un'altra 5.
Restano così definite le due applicazioni C_k :
la prima è $C_k : Z_{21} \to Z_{21}$

$$p \to 3 \cdot p + 4$$

la seconda è $C_k : Z_{21} \to Z_{21}$

$$p \to 5 \cdot p + 4$$

Visualizziamo in una tabella i risultati della cifratura:

Posiz. Lettera	Funz. 5p+4	Funz. 3p+4	Posiz. Lettera	Funz. 5p+4	Funz. 3p+4	Posiz. lettera	Funz. 5p+4	Funz. 3p+4
0 a	4	4	7 h	18	4	14 q	11	4
1 b	9	7	8 i	2	7	15 r	16	7
2 c	14	10	9 l	7	10	15 s	0	10
3 d	19	13	10 m	12	13	17 t	5	13
4 e	3	16	11 n	17	16	18 u	10	16
5 f	8	19	12 o	1	19	19 v	15	19
6 g	13	1	13 p	6	1	20 z	20	1

Si vede, quindi, che la funzione
$C_k : Z_{21} \to Z_{21}$

$$p \to 5 \cdot p + 4$$

è biunivoca, in quanto ad ogni lettera dell'alfabeto in chiaro resta associata una lettera diversa dell'alfabeto cifrato, ma questo non avviene con l'altra funzione

$$C_k : Z_{21} \to Z_{21}$$
$$p \to 3 \cdot p + 4$$

Allora possiamo concludere che in generale la funzione C_k non è biunivoca, ma per alcuni numeri la corrispondenza vale, per altri fallisce. È chiaro che non si può andare per tentativi nel decidere quali numeri possono andar bene e quali no, per questo sarà necessario studiare meglio le proprietà di Z_n e capire se esiste una regola generale per determinare, senza fare prove, se una funzione C_k è biunivoca, cioè se il sistema di cifratura che abbiamo formulato è realmente applicabile.