5.1 Il cifrario di Augusto

Supponiamo ad esempio di voler trasmettere il messaggio *ALESSANDRIA*. Come prima cosa trasformiamo il messaggio in una sequenza di numeri secondo la trasformazione *spazio* $\to 0$, $A \to 1$, $B \to 2$, $\ldots$, $Z \to 26$. Scegliamo poi una *chiave* ad esempio la parola *CIAO*. Scriviamo poi la codifica numerica del messaggio e sotto di essa la codifica numerica della chiave ripetuta più volte in modo da ottenere tanti valori quanti quelli presenti nel messaggio. Nel nostro esempio, dato che la codifica numerica di *CIAO* è $[3, 9, 1, 15]$, abbiamo

A	L	E	S	S	A	N	D	R	I	A
1	12	5	19	19	1	14	4	18	9	1
+ 3	9	1	15	3	9	1	15	3	9	1
4	21	6	7	22	10	15	19	21	18	2

Il messaggio cifrato è costituito dalla somma modulo 27 dei valori

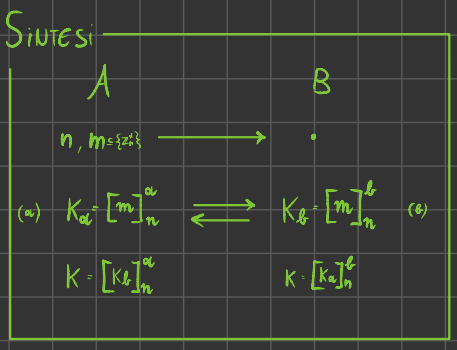
Nel nostro caso il messaggio cifrato è quindi $[4, 21, 6, 7, 22, 10, 15, 19, 21, 18, 2]$.

indicheremo questo algoritmo di crittografia con l'espressione "cifrario di Augusto, con chiave *CIAO*".

Definizione : Un algoritmo si dice efficiente se risolve un problema eseguendo un numero di operazioni aritmetiche che è al massimo proporzionale al logaritmo, o a una potenza del logaritmo, di uno dei dati di input.

PROTOCOLLO DIFFIE-HELLMAN:

permette a due computer di comunicarsi una chiave segreta in modo sicuro
(sfruttando il fatto che non esistono algoritmi efficienti per il calcolo del logaritmo discreto)



A	B
n, g: ① A prende un numero primo n (grande) e un numero (grande) in $\mathbb{Z}_n^*$: g	
② manda n e g a B	
③ A sceglie un numero a: $a < n-1$	③* B sceglie un numero b: $b < n-1$
K_a, K_b: ④ A manda a B K_a $\left(K_a = [g]_n^a\right)$	④* B manda ad A K_b $\left(K_b = [g]_n^b\right)$
⑤ A ha g, a, n e K_b	⑤* B ha g, a, n e K_a
⑥ TROVO CHIAVE: $K = [K_b]_n^a$	⑥* TROVO CHIAVE: $K = [K_a]_n^b$

C non può trovare la chiave perché non ha né a né b per calcolare la chiave dovrebbe fare un logaritmo discreto

essendo che non si scambiano i valori a, b