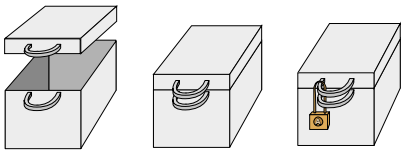
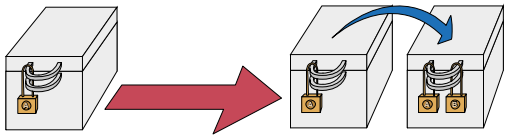
Il punto debole di ogni sistema crittografico visto finora è che esso presuppone l'esistenza di un canale e di un metodo sicuri per lo scambio della chiave. Nel contesto contemporaneo, nel quale la comunicazione avviene prevalentemente tra soggetti estranei (per esempio nelle transazioni via internet), lo scambio di chiavi preliminare non è possibile.

Il superamento del meccanismo della condivisione di chiave venne elaborato nel Novecento: esso viene spiegato quasi sempre attraverso l'analogia del doppio lucchetto, presentata qui sotto.

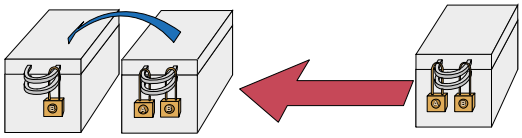
Una persona $\boxed{A}$ deve spedire un messaggio riservato a una persona $\boxed{B}$. Ripone quindi il testo in un bauletto e assicura quest'ultimo con un lucchetto. Nessuno al di fuori di $\boxed{A}$ può aprire ora la scatola.

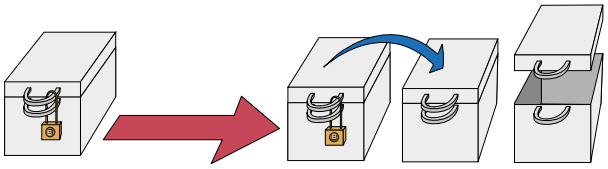




$\boxed{A}$ spedisce il bauletto a $\boxed{B}$ che però non lo può aprire. Lo sigilla quindi con un secondo lucchetto che nessun al di fuori di $\boxed{B}$ può manovrare.

A questo punto $\boxed{B}$ rispedisce il tutto ad $\boxed{A}$: questi può togliere il suo lucchetto.





$\boxed{A}$ rispedisce un ultima volta la scatola a $\boxed{B}$, che può ora aprire il suo lucchetto e quindi la scatola e leggere finalmente il messaggio.

Il meccanismo del doppio lucchetto prevede che il messaggio rimbalzi avanti e indietro tra i due interlocutori, operazione che non crea problemi con le infrastrutture telematiche contemporanee. Come si vede $\boxed{A}$ e $\boxed{B}$ non condividono alcuna chiave e il messaggio è sigillato in tutti e tre i viaggi.

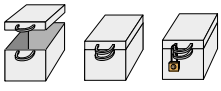
Cerchiamo ora di implementare quanto visto in chiave crittografica facendo applicare ad $\boxed{A}$ e a $\boxed{B}$ qualcuno dei sistemi che conosciamo:

Esempio 1

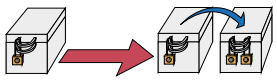
$\boxed{A}$ cifra per trasposizione a ZigZag con chiave "`partenza`"

$\boxed{B}$ cifra per sostituzione con un alfabeto traposto per chiave scalare "`arrivo`".

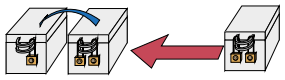
Il messaggio spedito da $\boxed{A}$ è "`Lucchetti, scatole e segreti`" cioè "`LUCCHETTISCATOLEESEGRETI`".



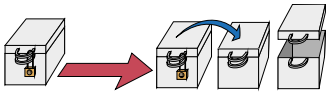
`LUCCHETTISCATOLEESEGRETI` → **`UTSSEHETIROLCIEECCTAEGLT`**



UTSSEHETIROLCIEECCTAEGLT → **FZTTWPWZXREMBXWWBBZAWLMZ**



FZTTWPWZXREMBXWWBBZAWLMZ → **MFBBPWZZXTBAZEMWWTWLRWZX**



MFBBPWZZXTBAZEMWWTWLRWZX → **LUCCHETTISCATOLEESEGRETI**

Come si vede è successo quanto auspicato: il messaggio "in viaggio" non è mai stato in chiaro, i due interlocutori non si sono sambiati alcuna chiave a al destinatario è giunto il messaggio corretto "Lucchetti, scatole e segreti". Non solo $\boxed{A}$ e $\boxed{B}$ non hanno mai conosciuto l'uno la chiave dell'altro, l'impressione è che ignorassero anche il sistema crittografico adoperato dal compagno.

Il prossimo esempio mostra che le cose non sono sempre così semplici.

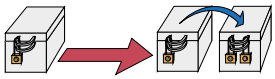
Esempio 2

$\boxed{A}$ cifra per trasposizione con la chiave scalare "`partenza`"

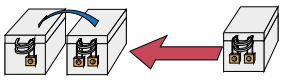
$\boxed{B}$ cifra per trasposizione a *ZigZag* con la chiave "`arrivo`".

Mandiamo quindi il messaggio "`Sono a casa, tutto bene!`"

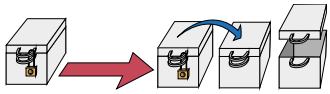
SONOACASATUTTOBENE → **ESNOENOAATTCUOASTB**



ESNOENOAATTCUOASTB → **EOOUTNSCSBANEAOATT**



EOOUTNSCSBANEAOATT → **OUNSSNOACBETAATEOT**



OUNSSNOACBETAATEOT → **OOAUNTNEOSAASTTCBE**

Come si vede stavolta il messaggio giunto a $\boxed{B}$ è sottosopra e un attento osservatore noterà che è arrivato in forma trasposta (si tratta cioè di un anagramma del messaggio originale). Perché è successo questo pasticcio?

Indicando con $A(m)$ il testo ottenuto applicando al messaggio m una certa cifratura A, con $B(m)$ una cifratura B e con $A^{-1}(m)$ e $B^{-1}(m)$ la rispettive "retrocifrature", si ha evidentemente che $A^{-1}(A(m))$ e $B^{-1}(B(m))$, perché per definizione la retrocifratura di una cifratura restituisce il messaggio originario. Quello che stiamo facendo noi è un'operazione un po' più complessa, che nella simbologia appena introdotta assumerebbe la seguente forma:

$$\boxed{B^{-1}\left(A^{-1}\left(B(A(m))\right)\right)}$$

Se potessimo scambiare fra loro le trasformazioni A^{-1} e B otterremmo $B^{-1}\left(B\left(A^{-1}(A(m))\right)\right)$, che , semplificato l'espressione dalla trasformazioni più interna, restituirebbe prima $B^{-1}\left(B(m)\right)$ e quindi m. Quando due trasformazioni possono essere scambiate nel loro ordine di esecuzione si dice che esse ***commutano***. Ebbene, la trasposizione e la sostituzione monoalfabetica commutano, mentre, in generale, due trasposizioni diverse non commutano: cambiare l'ordine di esecuzione ne modifica l'effetto.

10.1) Andando per istinto e buonsenso, indovina quale delle seguenti coppie di trasformazioni commutano e quali no. Espresso in termini meno matematici, stabilisci nei seguenti casi se il gioco del bauletto funzionerebbe (*nota bene: con la dizione Vigenère si intende il cifrario con gli alfabeti semplicemente slittati*). (*codice Kahoot:* **94956**)

	Metodo usato da A	Metodo usato da B	Commutano / non commutano
a)	*Cesare* con la misura dello slittamento per chiave (A)	*Cesare* con la misura dello slittamento per chiave (B)	
b)	Sostituzione monoalfabetica con chiave (A)	Sostituzione monoalfabetica con chiave (B)	
c)	Sostituzione monoalfabetica con chiave (A)	*Cesare* con la misura dello slittamento per chiave (B)	
d)	*Cesare* con la misura dello slittamento per chiave (A)	Trasposizione con chiave (B)	
e)	Trasposizione con chiave (A)	Trasposizione con chiave (B)	
f)	Vigenère con chiave (A)	Trasposizione con chiave (B)	
g)	Vigenère con chiave (A)	Vigenère con chiave (B)	
h)	Sostituzione monoalfabetica con chiave (A)	Vigenère con chiave (B)	

Generalmente commutano trasformazioni che agiscono su due caratteristiche indipendenti del testo come la posizione dei caratteri e i rappresentazione degli stessi (trasposizione→sostituzione). Il cifrario di Cesare (traposizione per slittamento) è una trasformazione molto particolare che commuta con se stessa: essa è alla

base della trasformazione (semplice) di Vigenère, anch'essa "autocommutante": quest'ultima circostanza è anzi abbastanza sorprendente.

Fino ad ora abbiamo "subito" i sistemi e il loro commutare non è dipeso da nostre scelte. Una volta sposata la filosofia del bauletto, si possono però inventare sistemi crittografici che commutino perché appositamente costruiti in modo che lo facciano.

Il prossimo esercizio, molto ambizioso, è che voi stessi riusciate ad inventare teniche crittografiche che possano essere usate nel protocollo a doppio lucchetto. Per facilitarvi il compito, ecco due semplici esempi:

Esempio 1
Supponiamo che $\boxed{A}$ cifri con un sistema qualsiasi tutte le lettere dispari del messaggio e $\boxed{B}$ cifri, a sua discrezione, tutte le lettere pari: sicuramente queste due trasformazioni commutano. Si tratterebbe tra l'altro di una strategia che non garantisce alcuna sicurezza: sapresti spiegare perché?

Esempio 2
Il secondo esempio parte da una certa trasposizione dal periodo possibilmente lungo che i due interlocutori condividono o conoscono entrambi (può benissimo trattarsi di una traposizione pubblica o di una regola comunicata attraverso un canale insicuro, per cui non deve essere considerata al pari di una chiave). La chiavi di cifratura usate separatemente dai due interlocutori sono il numero di iterazioni della trasposizione stessa. Ad esempio se le chiavi usate sono rispettivamente 104 e 3242, $\boxed{A}$ cifrerà usando la centoquattresima iterazione della traposizione e $\boxed{B}$ la tremiladuecentoquarantaduesima. Le due cifrature commutano.

10.2) Mettiti in gruppo (3-4 persone) e cerca di inventare assieme ai tuoi compagni una trasformazione compatibile con il doppio lucchetto e possibilmente sicura.

Abbiamo accennato prima al fatto che il protocollo del doppio lucchetto proposto nell'esempio **1** non dà garanzie di sicurezza. Vediamo il perché osservando il seguente "rimpallo":

Intercettando la "Trasmissione 1" `MIAOOODESA` si ottiene un messaggio nel quale ogni lettera pari è ancora in attesa della cifratura di $\boxed{B}$, intercettando invece la "Trasmissione 3" "`CXAWCSMVVO`" si ha a disposizione un testo nel quale ogni lettera dispari è già stata decifrata da $\boxed{A}$. Basterà quindi estrarre la parte non cifrata e quella già decifrata e reinserirle "a pettine":

TRASMISSIONE 1	M	**I**	A	**O**	O	**O**	D	**E**	S	**A**
TRASMISSIONE 3	**C**	X	**A**	W	**C**	S	**M**	V	**V**	O
MESSAGGIO IN CHIARO	**C**	**I**	**A**	**O**	**C**	**O**	**M**	**E**	**V**	**A**

Il fatto che uno stesso messaggio viaggi tre volte sullo stesso canale è un punto debole del protocollo a doppio lucchetto che può esser sfruttato da un intercettatore attraverso un'analisi differenziale, cioè confrontando lo stesso testo prima e dopo ogni "rimpallo". Vediamo a proposito un esempio basato sul protocollo $SOST \rightarrow TRASP$:

Trasmissione	Trasformazione	Cifratura	Messaggio trasmesso
1	A	Sostituzione monoalf.	ZPWPXSVAOUXTEYEZAYZX
2	B	Trasposizione	PZATXPWSOZXEUVXYAYEZ
3	A^{-1}	retroSostituzione	RTASIREMLTIOZBINANOT

Confrontiamo ora gli ultimi due testi: sappiamo che la terza trasmissione è frutto di una retrocifratura della prima sostituzione. Confrontando quindi lettera per lettera possiamo compilare una parte della "tabella del decifratore":

TABELLA DEL DECIFRATORE (o *TABELLA DI DECIFRAZIONE*)

Alfabeto CIFRATO	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto CHIARO	**A**				**O**										**L**	**R**			**M**	**S**	**Z**	**B**	**E**	**I**	**N**	**T**

Applicando questa tabella al primo messaggio siamo in grado decifrare il messaggio (il fatto che la tabella parziale ricostruita sopra sia sufficiente è una conseguenza della seconda tecnica usata: la trasposizione ha mischiato le lettere ma non ne ha introdotte altre):

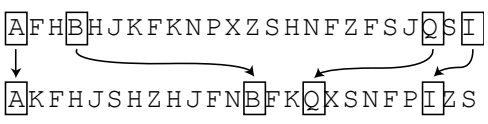
ZPWPXSVAOUXTEYEZAYZX → **TRERIMBALZISONOTROPPI**

Il messaggio originale è quindi "Tre rimbalzi sono troppi".

Vediamo ora un caso simile, nel quale però trasposizione e sostituzione sono state invertite:

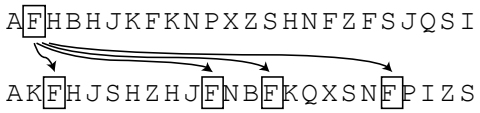
Trasmissione	Trasformazione	Cifratura	Messaggio trasmesso
1	A	Trasposizione	QESASTUEUMGPIOSMEIEOTNOL
2	B	Sostituzione monoalf.	AFHBHJKFKNPXZSHNFZFSJQSI
3	A^{-1}	retroTrasposizione	AKFHJSHZHJFNBFKQXSNFPIZS

Di nuovo confrontiamo gli ultimi due messaggi: i simboli che occorrono una volta soltanto permettono di abbozzare la tabella di permutazione della *retroTrasposizione* (a fianco sono mostrati soltanto quattro dei sei casi individuati in basso):



		A	F	H	B	H	J	K	F	K	N	P	X	Z	S	H	N	F	Z	F	S	J	Q	S	I
Posizione di partenza	↓	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Posizione di arrivo		1			13							21	17										16		22
		A	K	F	H	J	S	H	Z	H	J	F	N	B	F	K	Q	X	S	N	F	P	I	Z	S

Per altre lettere restano aperte più possibilità, come mostrato a fianco (→).



Complessivamente esistono $1! \cdot 4! \cdot 3! \cdot 1! \cdot 2! \cdot 2! \cdot 2! \cdot 1! \cdot 1! \cdot 2! \cdot 3! \cdot 1! \cdot 1! = 13.824$ trasposizioni compatibili con le ultime due trasmissioni (valore ottenuto calcolando il prodotto del numero delle permutazioni interne dei gruppi delle lettere ripetute). Per trovare la combinazione esatta sarà necessario analizzare il testo della prima trasmissione, applicare la traccia di permutazione inversa e valutare il risultato (per i curiosi il messaggio trasmesso era "`Questo sistema è un po' meglio`"). Se il numero 13.824 vi sembra grande, considerate che la stringa `AKFHJSHZHJFNBFKQXSNFPIZS` ha $89.763.947.010.017.280.000$ permutazioni diverse, un numero 6 milioni di miliardi volte maggiore di 13.824.

Abbiamo così potuto osservare come l'ordine delle tecniche del protocollo a doppio lucchetto influenzi sensibilmente la sicurezza complessiva del metodo e che "l'anello debole" della catena è la tecnica crittografica usata da $\boxed{A}$: ciò non sorprende, dal momento che la trasformazione di $\boxed{A}$ è l'unica ad essere tanto applicata quanto retroapplicata sul canale pubblico. Vediamo come ve la cavate voi:

10.3) Una trasmissione a doppio lucchetto del tipo $Sostituzione \rightarrow Trasposizione \rightarrow retroSostituzione \rightarrow retroTrasposizione$ viene intercettata in tutte e tre le trasmissioni. Determina il contenuto del messaggio:

Trasmissione	Trasformazione	Cifratura	Messaggio trasmesso
1	A	Sostituzione monoalf.	`KFAPAYZAKFAZZPEGAZZX`
2	B	Trasposizione	`PKAZAFAYKGXZFZAPAZEZ`
3	A^{-1}	retroSostituzione	`RQATAUANQGITUTARATOT`

Generazione speculare di chiave senza scambio

Quanto visto dovrebbe convincerci della necessità di superare anche il protocollo del doppio lucchetto: l'assenza dello scambio della chiave ha mostrato lasciare scoperto un altro angolo del velo crittografico.

Per capire come procedere consideriamo il seguente esempio, tratto dalle slide online del prof. Danielli dell'Univeristà di Ferrara (https://slideplayer.it/slide/14832114/)

Supponiamo di vivere in un mondo in cui tutti sanno moltiplicare ma nessun sa dividere. L'incapacità di rendere reversibile un'operazione matematica (in questo caso la moltiplicazione) può essere usata non già per scambiarsi una chiave, ma per permettere ai due interlocutori di crearsene una, ciascuno "a casa propria", in modo che il risultato sia identico.

Vediamo come fare attraverso il seguente esempio e immaginiamo come al solito che $\boxed{A}$ e $\boxed{B}$ vogliano comunicare tra loro in modo sicuro. Decidono quindi di operare "alla vecchia maniera", cioè senza adottare il protocollo del doppio lucchetto: si pone quindi il solito problema dello scambio della chiave $\boxed{A}$ e $\boxed{B}$ in presenza di un intercettatore malintenzionato che chiamiamo $\boxed{M}$. Vediamo la strategia adottata da $\boxed{A}$ e $\boxed{B}$:

$\boxed{A}$ manda a $\boxed{B}$ un numero N, poniamo $N = 97$.	→	$\boxed{M}$ intercetta 97
$\boxed{B}$ sceglie un proprio numero privato, poniamo $b = 19$. Questo numero non deve assolutamente essere intercettato: per "coprirlo", $\boxed{B}$ calcola il prodotto $Nb = 1843$ e lo trasmette ad $\boxed{A}$.	→	$\boxed{M}$ intercetta 1843
Anche $\boxed{A}$ sceglie un proprio numero privato, poniamo $a = 47$ che non divulga. Spedisce quindi a $\boxed{B}$ il prodotto $Na = 4559$.	→	$\boxed{M}$ intercetta 4559

A questo punto della storia sono transitati tra $\boxed{A}$ e $\boxed{B}$ ben 3 dati, tutti e tre intercettati da $\boxed{M}$

Prima trasmissione	Seconda e terza trasmissione (avvenute contemporaneamente)	
$\boxed{A} \overset{97}{\rightarrow} \boxed{B}$	$\boxed{B} \overset{1843}{\longrightarrow} \boxed{A}$	$\boxed{A} \overset{4559}{\longrightarrow} \boxed{B}$

$\boxed{M}$ conosce non solo i tre numeri 97, 1843 e 4559, ma anche il loro significato: sa cioè che 1843 è uguale a 97 per "qualcosa" e 4559 è 97 per "qualcos'altro". Non sapendo come si svolge la divisione, $\boxed{M}$ non può però determinare né il valore di "qualcosa" né di "qualcos'altro" (si tratta dei due numeri privati a e b). Anche $\boxed{A}$ e $\boxed{B}$ sono vittime della stessa ignoranza e non sono in grado di conoscere il numero privato nel compagno.

Come anticipato, $\boxed{A}$ e $\boxed{B}$ lavorano ora, ciascuno a casa propria, alla creazione di una chiave (che non hanno scelto a monte ma che ottengono con un calcolo).

$\boxed{A}$ effettua la moltiplcazione $\boxed{Nb \cdot a}$ e ottiene $1843 \cdot 47 = \boxed{86.621}$	→	In questa fase non avvengono trasmissioni
$\boxed{B}$ effettua la moltiplcazione $\boxed{Na \cdot b}$ e ottiene $= 4559 \cdot 19 = \boxed{86.621}$	→	

La commutatitivà della moltiplicazione assicura che il risultato sarà lo stesso (abN). Il numero potrà quindi essere usato da entrambi come chiave per effettuare in seguito una comunicazione sicura tramite una della tecniche crittografiche studiate. Da notare che nessuno dei due interlocutori conosce né conoscerà mai il numero "segreto" del compagno.

La condizione dell'intercettatore $\boxed{M}$ è la seguente: egli conosce N, Na e Nb e vorrebbe impossessarsi della chiave comune abN. $\boxed{M}$ è però in grado di moltiplicare ma non di dividere, riesce quindi a ricavare valori come $N \cdot Na = aN^2$, $N \cdot Nb = bN^2$, $Na \cdot Nb = abN^2$ ma non abN!

Il metodo appena descritto si basa due ipotesi:

- l'operazione è commutativa per cui A e B otterranno lo stesso risultato
- l'operazione non è facilmente invertibile (se vi ricordate, si era assunto in premessa di vivere in un mondo privo dell'operazione di divisione)

L'avverbio "facilmente" usato a proposito dell'invertibilità sottolinea che si tratta di un'ostacolo tecnico e non di un'impossibilità teorica: andando a tentativi ed effettuando in ordine tutte le moltiplicazioni, prima o poi si troverà il fattore corretto (anche non sapendo nulla di divisioni).

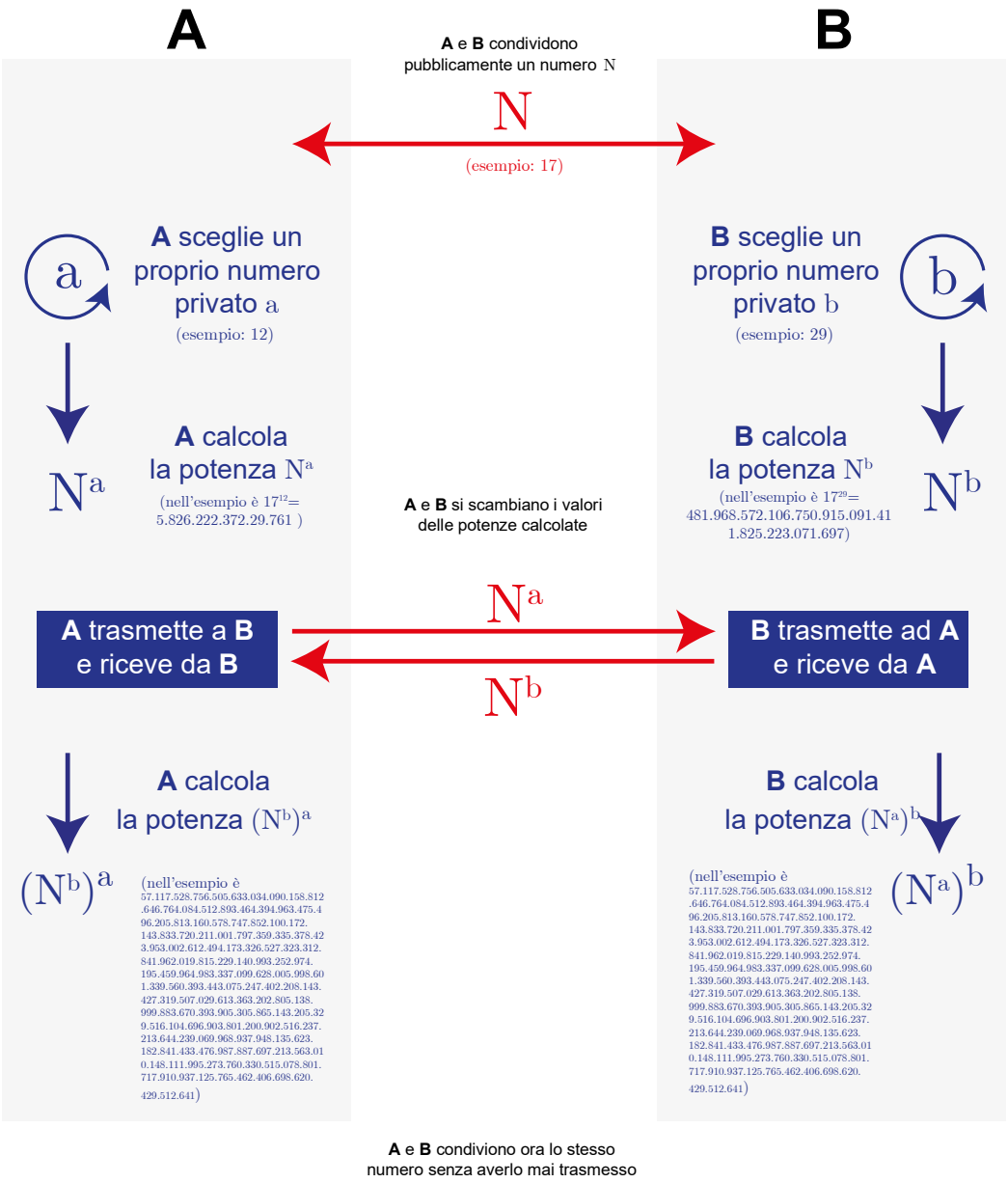
10.4) Prima di passare al "mondo reale" promesso sopra, consideriamo una modifica all'algoritmo precedente: la moltiplicazione per le chiavi private è sostituita dall'elevamento a potenza di base N. Studiando il procedimento descritto in basso, si riconosce facilmente che la commutatività è garantita. Per quanto riguarda la difficoltà dell'inversione, cosa ne pensate?

$\boxed{A}$ manda a $\boxed{B}$ un numero N, poniamo $N = 17$.	→	$\boxed{M}$ intercetta 17
$\boxed{B}$ sceglie un proprio numero privato, poniamo $b = 29$, calcola N^b, cioè $481.968.572.106.750.915.091.411.825.223.071.697$ e lo trasmette.	→	$\boxed{M}$ intercetta N^b
$\boxed{A}$ sceglie un proprio numero privato, poniamo $a = 12$, calcola N^a, cioè $5.826.222.372.29.761$ e lo trasmette.	→	$\boxed{M}$ intercetta N^a
$\boxed{A}$ effettua l'elevamento a poteza $(N^b)^a$ e ottiene N^{ab} (spaventoso numero rappresentato in basso).	→	In questa fase non avvengono trasmissioni
$\boxed{B}$ effettua l'elevamento a poteza $(N^a)^b$ e ottiene nuovamente N^{ab}.	→	

$17^{(12\cdot 29)} = 17^{348} =$

$57.117.528.756.505.633.034.090.158.812.646.764.084.512.893.464.394.963.475.496.205.813.160.578.747.852.100.172.$
$143.833.720.211.001.797.359.335.378.423.953.002.612.494.173.326.527.323.312.841.962.019.815.229.140.993.252.974.$
$195.459.964.983.337.099.628.005.998.601.339.560.393.443.075.247.402.208.143.427.319.507.029.613.363.202.805.138.$
$999.883.670.393.905.305.865.143.205.329.516.104.696.903.801.200.902.516.237.213.644.239.069.968.937.948.135.623.$
$182.841.433.476.987.887.697.213.563.010.148.111.995.273.760.330.515.078.801.717.910.937.125.765.462.406.698.620.$
$429.512.641$

Vediamo qui in basso un riassunto del metodo appena descritto



Voi siete alunni del biennio del Liceo Scientifico e questo implica che non avete ancora familiarizzato con tutte frecce contenute nella faretra "standard" del matematico, tra le quali spicca il **logaritmo**. Si tratta a tutti gli effetti della tecnica di inversione del metodo delle potenze visto sopra e con una calcolatrice è facilissimo ottenere l'esponente ignoto in quattro e quattro otto. Nonostante questa vostra mancanza, quello che sapete sui radicali e sulle potenze con esponente frazionario è sufficiente per invertire le operazioni viste sopra, dal momento che esse sono basate esclusivamente su potenze tra numeri interi. Vediamo un esempio e consideriamo la relazione $17^b = 481.968.572.106.750.915.091.411.825.223.071.697$ (equazione che vorrebbe risolvere l'intercettatore del messaggio precedente). Per trovare b non è necessario che l'intercettatore provi tutti le potenze del 17, è sufficiente che egli "si avvicini" a una potenza del 10, come mostrato in basso.

$$17^{13} = 9.904.578.032.905.937 \cong 10^{16} \text{ cioè } 10 \cong \sqrt[16]{17^{13}} = 17^{\frac{13}{16}}$$

Avere approssimato il 17 con una potenza frazionaria del 10 permette ora di sveltire i calcoli: contando le cifre del numero $481.968.572.106.750.915.091.411.825.223.071.697$ sicuramente vale la doppia disugliuanza

$$10^{35} < 481.968.572.106.750.915.091.411.825.223.071.697 < 10^{36}$$

…che, prendendo per buona l'approssimazione $10 \cong 17^{\frac{13}{16}}$, possiamo trasformare in…

$$\left(17^{\frac{13}{16}}\right)^{35} < 481.968.572.106.750.915.091.411.825.223.071.697 < \left(17^{\frac{13}{16}}\right)^{36}$$

…e quindi….

$$17^{28,4} < 481.968.572.106.750.915.091.411.825.223.071.697 < 17^{29,3}$$

A questo punto è immediato concludere che l'esponente cercato è 29. Notiamo che approssimazioni peggiori di $10 \cong 17^{13/16}$ avrebbero comunque consentito di restringere il campo di ricerca. Dalla relazione grossolana $17^4 = 83.521 \cong 10^5$ e quindi $10 \cong 17^{4/5}$ saremmo per esempio arrivati alla doppia disequazione $17^{28} < \cdots < 17^{28,8}$, evidentemente falsa (l'approssimazione iniziale era fin troppo rozza) ma comunque sufficiente ad indirizzarci verso l'ordine di grandezza corretto.

10.5) Sopponi che 53^x con $x \in \mathbb{N}$ sia un numero di un milione di cifre. Sapendo che $53^{29} \cong 10^{50}$ approssima il valore di x.

Ora che abbiamo esplorato la possibilità di sostituire lo scambio della chiave con la creazione speculare della stessa (quindi senza alcuno scambio intercettabile) in un mondo irreale nel quale nessuno conosce divisione o logaritmo, dobbiamo chiederci se è possibile trovare qualcosa di adatto nel mondo reale, cioè un'operazione che sia……

- **commutativa** (il che consentirà ad A e B di generare la stessa chiave)
- **proibitiva da invertire** (in modo che l'intercettatore non possa ricavare i numeri privati)

La commutatività non sembra una caratteristica difficile da ottenere (la Matematica pullula di trasformazioni del genere), l'obiettivo difficile da centrare pare il secondo. Esso può essere realizzato utilizzando le cosiddette *funzioni unidirezionali*:

Le funzioni unidirezionali

Consideriamo i due polinomi $P(x)$ e $Q(x)$ incorniciati in basso:

$$P(x) = 27(2x-3)^3\left(2x+\frac{4}{3}\right)\left(x-\frac{11}{9}\right)(x-1)\,(x^2+5)$$

$$Q(x) = 432x^8 - 2616x^7 + 7988x^6 - 18.218x^5 + 29.068x^4 - 22.936x^3 - 1548x^2 + 13.770x - 5940$$

Quali sono gli zeri di $P(x)$? Evidentemente $x_1 = 3/2$, $x_2 = -2/3$, $x_3 = 11/9$, $x_4 = 1$. Stabilire gli zeri di $Q(x)$ è invece piuttosto difficile: non esiste infatti una formula generale (per radicali) che consenta di trovare gli zeri esatti di un polinomio dal quarto grado in su, risolvere l'equazione $Q(x) = 0$ non è quindi alla nostra portata. Portando $P(x)$ in forma normale (cioè svolgendo i calcoli), si vede però che $P(x)$ è proprio $Q(x)$, per cui anche

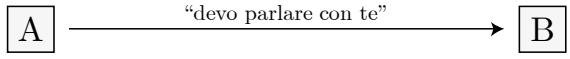
$Q(x)$ ha gli zeri $x_1 = 3/2,\ x_2 = -2/3, x_3 = 11/9, x_4 = 1$ (i più scettici possono verificarlo numericamente, perlomeno nel caso più semplice $x_4 = 1$).

Moltiplicare i fattori di un polinomio scomposto è come spingere il dentifricio fuori dal tubetto, un'operazione molto facile da svolgere in un senso e proibitiva (o impossibile) nell'altro: in pratica, svolgere la moltiplicazione ha avuto l'effetto di "crittare" gli zeri del polinomio. Le operazioni che sono molto difficili da invertire si chiamano **funzioni unidirezionali** o **funzioni a senso unico** e, come vedremo, in Matematica se ne incontrano parecchie. Un altro termine largamente usato per definire le *funzioni unidirezionali* è **trasformazioni asimmetriche**: nel caso succitato, moltiplicazione di polinomi e loro fattorizzazione sono le due *trasformazioni asimmetriche*.

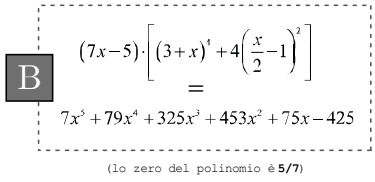
Riagganciandoci al binomio asimmetrico moltiplicazione-fattorizzazione considerate il protocollo di generazione di chiavi descritto in basso: si tratta di un sistema poco sicuro (come verrà spiegato in seguito) ed è citato soltanto a titolo di esempio.

Algoritmo basato sullo "zero del polinomio"

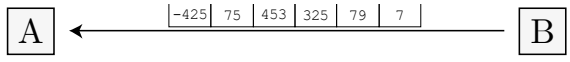
$\boxed{A}$ vuole mandare a $\boxed{B}$ un certo numero intero K (potrebbe trattarsi di una chiave che i due vogliono usare per future comunicazioni). $\boxed{A}$ avverte quindi $\boxed{B}$ della sua intenzione e gli chiede di mandargli un *vettore* su cui far viaggiare l'informazione.



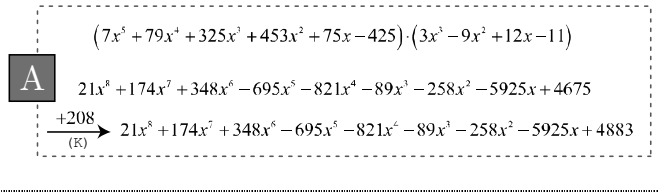
$\boxed{B}$ costruisce il *polinomio vettore* $B(x)$: si tratta di un polinomio di zero Z che $\boxed{B}$ "nasconde" eseguendo un qualche prodotto in modo da ottenere un polinomio di grado maggiore di 4.



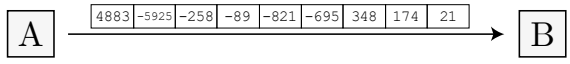
$\boxed{B}$ trasmette ad $\boxed{A}$ i coefficienti del polinomio $B(x)$, rispettando un ben preciso ordine e non dimenticando eventuali zeri per eventuali monomi nulli. A fianco si è partiti dal termine noto.



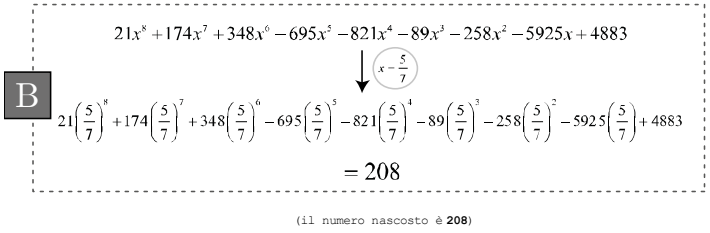
$\boxed{A}$ ricostruisce il polinomio $B(x)$ e lo moltiplica per un polinomio "arbitrario" $A(x)$, necessario a "mischiare le carte". A questo punto somma il numero K, ottenendo il polinomio $P(x) = A(x)B(x) + K$.



$\boxed{A}$ spedisce a $\boxed{B}$ i coefficienti di $P(x)$. K è ora nascosto nel termine noto di $P(x)$. Visto che $\boxed{M}$ non conosce $A(x)$, non può ricavare il valore di K.



$\boxed{B}$ riceve i coefficienti di $P(x)$ e calcola $P(Z)$, cioè inserisce al posto di x il valore Z. Quello che otterrà sarà proprio K (infatti visto che $B(Z) = 0$ si ha $P(Z) = A(Z)B(Z) + K = A(Z) \cdot 0 + K = K$)



Le intercettazioni permettono al malintenzionato $\boxed{M}$ di conoscere $B(x)$ e $P(x)$, teoricamente gli restano preclusi tanto $A(x)$ che Z, dati indispensabili per calcolare K.

Questa tecnica ha molti punto deboli, legate tanto alla "copertura" di $A(x)$ quanto a quella Z. Per trovare K non è infatti indispensabile conoscere Z con precisione assoluta, è sufficiente una sua buona approssimazione (il che non costituisce alcun problema per un matematico, indipendentemente dal grado del polinomio). Il lato $A(x)$ è ancora più scoperto: si possono facilmente ricostruire ricorsivamente i coefficienti di $A(x)$ a partire da quelli di $B(x)$ e $P(x)$. Insomma, l'algoritmo dello "zero del polinomio" non va bene, serve un'idea migliore!

Algoritmo di Diffie-Hellman

Torniamo ora al metodo della chiave speculare con le potenze e cerchiamo di lavorare sulla sua invertibilità (cerchiamo cioè di renderlo asimmetrico). Nei calcoli precedenti eravamo riusciti ad invertire il meccanismo cifrante senza nemmeno conoscere il logaritmo, operazione matematica a ciò preposta: la nostra strategia si basava esclusivamente su considerazioni quantitative, tradotte poi in disequazioni.
Un modo per spuntare l'arma dell'analisi quantitativa è introdurre dei meccanismi matematici che spezzino il legame fra grandezza dell'esponente e grandezza della potenza: la scelta aritmeticamente più ovvia (vedremo dopo perché) è quella di considerare i resti prodotti da divisioni con quoziente anziché i numero "grezzi". Per realizzare ciò è importante che i due interlocutori condividano inizialmente non solo il numero N (base delle varie potenze) ma anche un altro intero p, primo a N (per cui il massimo comun divisore tra p e N è 1) che verrà utilizzato come divisore.

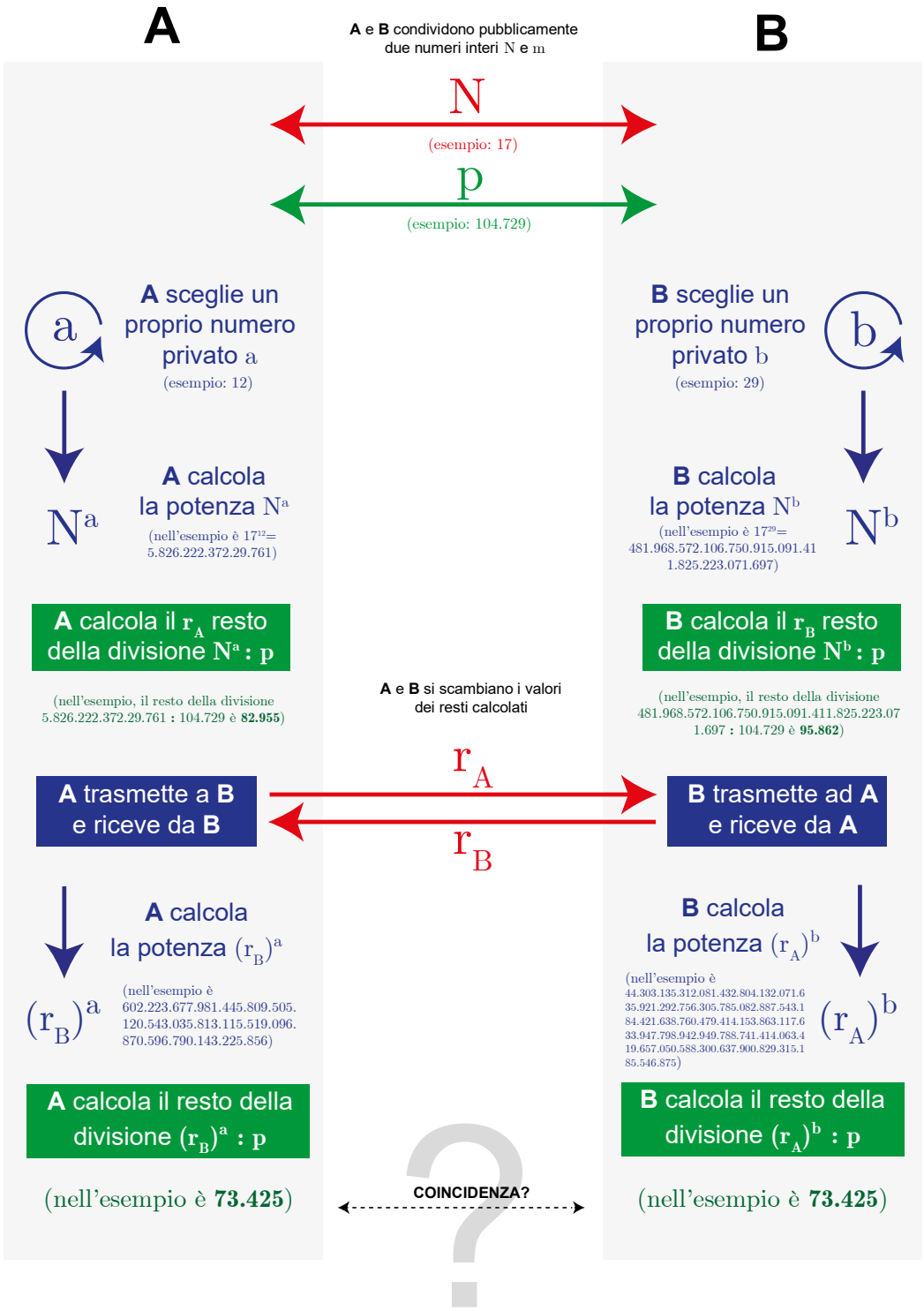
Per introdurre il concetto del resto, prendiamo l'ultimo numero "mostro" creato nell'esempio delle potenze:

57.117.528.756.505.633.034.090.158.812.646.764.084.512.893.464.394.963.475.496.205.813.160.578.747.852.100.172.143.833.
720.211.001.797.359.335.378.423.953.002.612.494.173.326.527.323.312.841.962.019.815.229.140.993.252.974.195.459.964.983.
337.099.628.005.998.601.339.560.393.443.075.247.402.208.143.427.319.507.029.613.363.202.805.138.999.883.670.393.905.
305.865.143.205.329.516.104.696.903.801.200.902.516.237.213.644.239.069.968.937.948.135.623.182.841.433.476.987.887.
697.213.563.010.148.111.995.273.760.330.515.078.801.717.910.937.125.765.462.406.698.620.429.512.641

I due interlocutori potrebbero non avere bisogno di una chiave tanto lunga, decidono quindi di scambiarsi un altro intero $p = 104.729$, di dividere il "mostro" per p e di utilizzare il resto (un numero compreso tra 0 e $p - 1$) come chiave condivisa. Nell'esempio specifico otterrebbero 73.425, un numero che è bene tenere a mente. È opportuno osservare che questo procedimento non migliora affatto la segretezza del metodo delle potenze, dal momento che questo passaggio al resto avviene soltanto "a babbo morto", cioè a trasmissioni avvenute.

Immaginiamo quindi che tutti i valori calcolati dai due interlocutori, anche quelli relativi alle comunicazioni iniziali, vengano sottoposti a una divisione (intera) per p e che i soli numeri trasmessi siano i resti di tali divisioni.

Per chiarire il meccanismo ecco qui lo schema: in verde le aggiunte rispetto allo schema precedente.



Come si vede, sorprendentemente i conti tornano e anzi, il numero 73.425 è proprio l'intero che avevamo ottenuto dividendo "il mostro" per p: a meno di una incredibile coincidenza, pare che svolgere i calcoli con i resti o svolgere i calcoli con i numeri "grezzi" produca lo stesso risultato. Prima di fare altri tentativi e presentare la matematica a sostegno di quanto visto, è bene citare gli informatici che hanno ideato questo sistema, presentandolo al pubblico in una conferenza del 1976: si tratta di Whit Diffie e Martin Hellman.

Dividetevi ora a coppie e provate voi, ciascuno con il suo numero segreto, a generare chiavi speculari. Per simulare il metodo in modo corretto, è importante che vi comunichiate soltanto i dati che nella tabella in basso stanno nelle colonne bianche (cioè $N, p, r_A(resto)$ e $r_B(resto)$)

N	p	a	N^a	$r_A\ (resto)$	r_A^b	$(resto)$	b	N^b	$r_B\ (resto)$	r_B^a	$(resto)$

a)	7	31										
b)	10	9										
c)	3	20										
d)	11	10										
e)	9	5										
f)	2	11										

La matematica “dei resti” si chiama **Aritmetica Modulare**, ed è una parte importantissima del calcolo discreto, cioè della matematica dei numeri interi (detta anche Teoria dei Numeri o semplicemente Aritmetica). In questo periodo storico, l’aritmetica modulare sta trovando proprio della Crittografia e nell’Informatica una inaspettata seconda giovinezza.

Vediamo un esempio applicativo dell’aritmetica modulare come strumento crittografico di trasposizione:

10.6a) Compila la griglia di destra seguendo le indicazioni scritte sulla freccia azzurra (ciascun numero va prima moltiplicato per 6 e poi sottoposto alla divisione intera per 25: nella cella va scritto il resto della divisione).

0	1	2	3	4
5	6	7	8	9
10	11	12	**13**	14
15	16	17	18	19
20	21	22	23	24

si moltiplica per 6 e si considera il resto nella divisione per 25

esempio:
13·6=78 e
78:25 dà resto 3

			3	

10.6b) Quale è il periodo della trasposizione precedente?