Azzolini Riccardo 2021-03-11

Tecniche di trasposizione e schemi a più fasi

1 Tecniche di trasposizione

La cifratura con tecniche di trasposizione si basa su una permutazione delle lettere del testo in chiaro, che vengono solo "spostate", senza modificarle. Allora, a differenza di quanto accade con le tecniche di sostituzione, la frequenza delle lettere rimane invariata dal testo in chiaro al testo cifrato, ma, in compenso, spostando le lettere si "spezzano" le strutture di più lettere presenti nel plaintext (digrammi, trigrammi, header di un file/protocollo, ecc.), che gli schemi di sostituzione tendono invece a preservare.

1.1 Rail fence

Una semplice esempio di tecnica di trasposizione è la **rail fence** ("staccionata"), che consiste nello scrivere il testo in chiaro come una sequenza di diagonali di una certa lunghezza, e poi leggere le lettere così disposte come una sequenza di righe per ottenere il testo cifrato. In questo schema, la chiave è la *profondità* della staccionata, cioè la lunghezza delle diagonali.

Ad esempio, dato il testo in chiaro

```
meet me after the toga party
```

per cifrarlo con profondità due esso viene disposto come

```
m   e   m   a   t   r   h   t   g   p   r   y
  e   t   e   f   e   t   e   o   a   a   t
```

e poi letto riga per riga, ottenendo:

```
MEMATRHTGPRYETEFETEOAAT
```

Questo schema può essere facilmente oggetto di attacchi a forza bruta, perché lo spazio delle chiavi è limitato dal fatto che le diagonali non possono essere più lunghe del messaggio, dunque un attaccante riuscirebbe facilmente a provare tutte le possibili lunghezze, fino a ottenere il testo in chiaro (purché, come al solito, sia in grado di riconoscere quest'ultimo per capire che la decifratura ha avuto successo).

1.2 Trasposizione di colonne

Uno schema più complesso consiste nello scrivere un messaggio riga per riga in una matrice, e poi leggerlo colonna per colonna, permutando però l'ordine delle colonne. L'ordine in cui leggere le colonne (e il numero di colonne) costituisce dunque la chiave.

Ad esempio, si considerino il testo in chiaro

```
attack postponed until two am
```

e la chiave `4 3 1 2 5 6 7`, nella quale ogni numero corrisponde a una colonna e indica la sua posizione nell'ordine di lettura. Per eseguire la cifratura, si dispone innanzitutto il plaintext riga per riga in una matrice avente tante colonne quanti sono i numeri che formano la chiave; se la lunghezza del messaggio non è un multiplo del numero di colonne, si aggiungono dei caratteri di riempimento prefissati (concordati con il destinatario del messaggio; qui ad esempio sono lettere `x`) per completare l'ultima riga:

Chiave:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	x	x

Il testo cifrato è poi ottenuto leggendo prima la colonna che la chiave ha numerato 1, dall'alto verso il basso, poi la colonna 2, e così via:

```
TTNAAPTMTSUOAODWCOIXKNLXPETX
```

Anche se questo schema è più complesso del rail fence, la crittoanalisi rimane abbastanza semplice: si dispone il testo cifrato su una matrice di larghezza corrispondente alla lunghezza della chiave ipotizzata e si prova a ricostruire l'ordine delle colonne.

Lo schema può essere reso più sicuro eseguendo la trasposizione più volte, in più fasi: una volta ottenuto il testo cifrato, lo si tratta di nuovo come se fosse un testo in chiaro da cifrare, con la stessa chiave o (meglio ancora) con una chiave diversa, e così via. Questo rende più difficile la ricostruzione, perché un attaccante non ha modo di capire subito quando la decifratura della prima fase ha avuto successo, ma piuttosto deve tentare tutte le fasi per ogni possibile chiave o combinazione di chiavi.

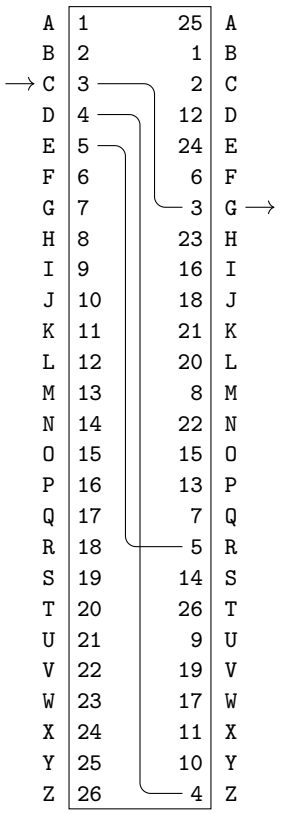
2 Schemi a più fasi

Il principio appena accennato nel contesto delle permutazioni vale in realtà anche per le sostituzioni: in generale, applicare una stessa primitiva di cifratura più volte, su più **fasi** o **round**, con la stessa chiave o con chiavi diverse, rende più difficili sia gli attacchi di brute force (perché l'esecuzione di ciascun tentativo di decifratura ha un costo maggiore) che quelli di crittoanalisi (perché la relazione tra il plaintext, la chiave e il ciphertext diventa più complicata).

2.1 Esempio: macchine a rotazione

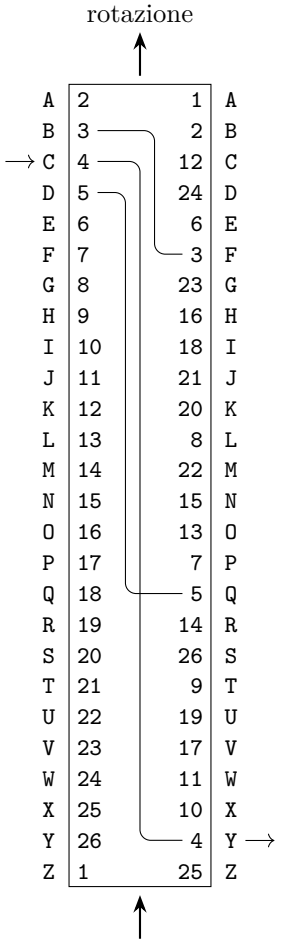
Un esempio di schema di cifratura basato su più fasi di sostituzione sono le *macchine a rotazione* (o *a rotori*), che furono molto usate durante la seconda guerra mondiale (la più famosa è la macchina Enigma impiegata dalla Germania, ma anche le altre nazioni avevano macchine simili).

Una macchina a rotazione è costituita da un certo numero di *cilindri* o *rotori*, ciascuno dei quali implementa in sostanza una sostituzione polialfabetica. Per una macchina che lavora su un alfabeto di 26 lettere, ogni cilindro ha 26 contatti elettrici di ingresso e 26 contatti di uscita; internamente al cilindro, ogni ingresso è cablato a un'uscita diversa, secondo uno schema fissato al momento della costruzione del cilindro. Se si associano a ogni ingresso e a ogni uscita una lettera dell'alfabeto, allora il cilindro esegue una sostituzione monoalfabetica:



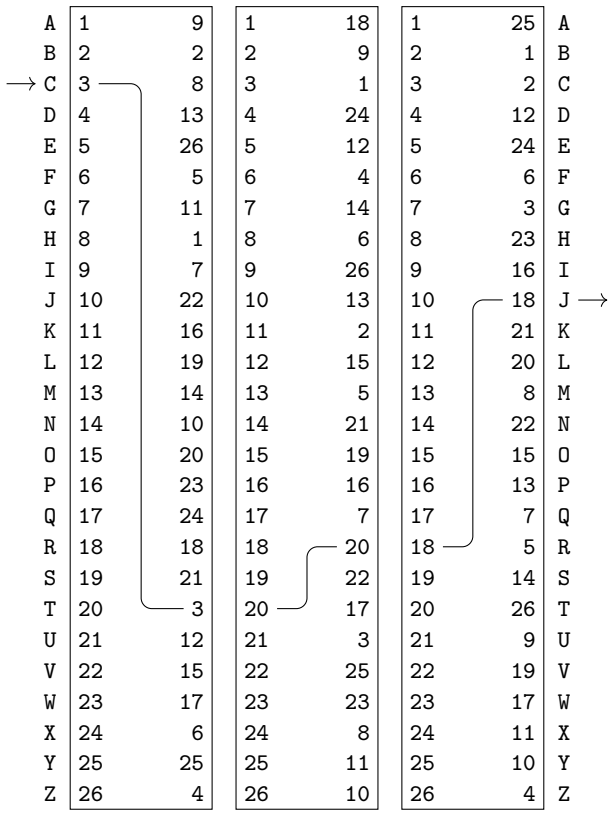
(per semplicità, qui sono rappresentati solo alcuni dei collegamenti tra ingressi e uscite, ma esiste un collegamento tra ogni coppia di ingresso e uscita etichettati con lo stesso numero).

A ogni pressione di un tasto della macchina, il cilindro ruota di una posizione, dunque cambiano le lettere associate a ciascun contatto, ovvero cambia la sostituzione eseguita:

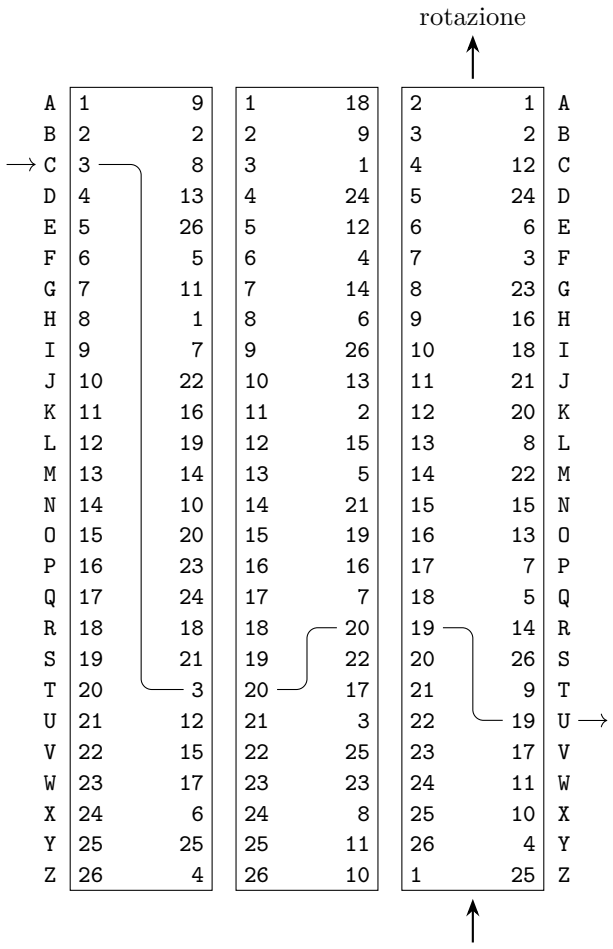


Di conseguenza, un cilindro rotante realizza una sostituzione polialfabetica che fa uso di un insieme di 26 sostituzioni monoalfabetiche.

Ora, per rendere il cifrario più efficace si applica l'idea di effettuare più fasi di sostituzione, aggiungendo ulteriori cilindri, disposti in modo che le uscite di ciascun cilindro siano collegate agli ingressi del cilindro successivo. Ad esempio, con tre cilindri si avrebbe una situazione del genere:



È molto importante il modo in cui questi cilindri girano. Infatti, se ruotassero tutti insieme a ogni pressione di un tasto, il numero di sostituzioni moloalfabetiche utilizzate sarebbe ancora solo 26: dopo 26 pressioni, tutti i cilindri tornerebbero alle loro posizioni iniziali. Invece, per fare in modo che vengano "esplorate" tutte le possibili combinazioni di posizioni dei cilindri, deve esserci un primo cilindro che gira di una posizione a ogni pressione,



un secondo cilindro che gira di una posizione ogni volta che il primo cilindro completa una rotazione di 26 posizioni, e così via, come le cifre di un contachilometri. In questo modo, ad esempio, con 3 cilindri si ottengono $26^3 = 17\,576$ sostituzioni monoalfabetiche diverse.

Le macchine a rotazione reali erano spesso ancora più complesse rispetto allo schema appena descritto. Ad esempio, nel caso della macchina Enigma a 3 rotori si avevano tipicamente a disposizione cinque rotori tra cui scegliere i tre da usare, dopodiché bisognava impostare la posizione iniziale di ciascun rotore, e infine c'era la possibilità di effettuare un'ulteriore sostituzione monoalfabetica, tramite dei cavi che potevano essere collegati in modo da scambiare coppie di lettere, sostituendo ciascuna lettera di una coppia con l'altra. Perciò, il numero di configurazioni diverse possibile era enorme.

3 Conclusioni

Riassumendo:

- le sostituzioni (non monoalfabetiche) celano la frequenza delle singole lettere;
- le trasposizioni spezzano le strutture di più lettere presenti nel ciphertext;
- lo svolgimento di più fasi di cifratura, soprattutto se fatto con una chiave diversa per ogni fase, permette di rendere più complesso e sicuro uno stesso schema di cifratura.

Perciò, gli algoritmi di crittografia simmetrica moderni sono tipicamente basati su schemi che combinano più fasi di sostituzione e di permutazione.