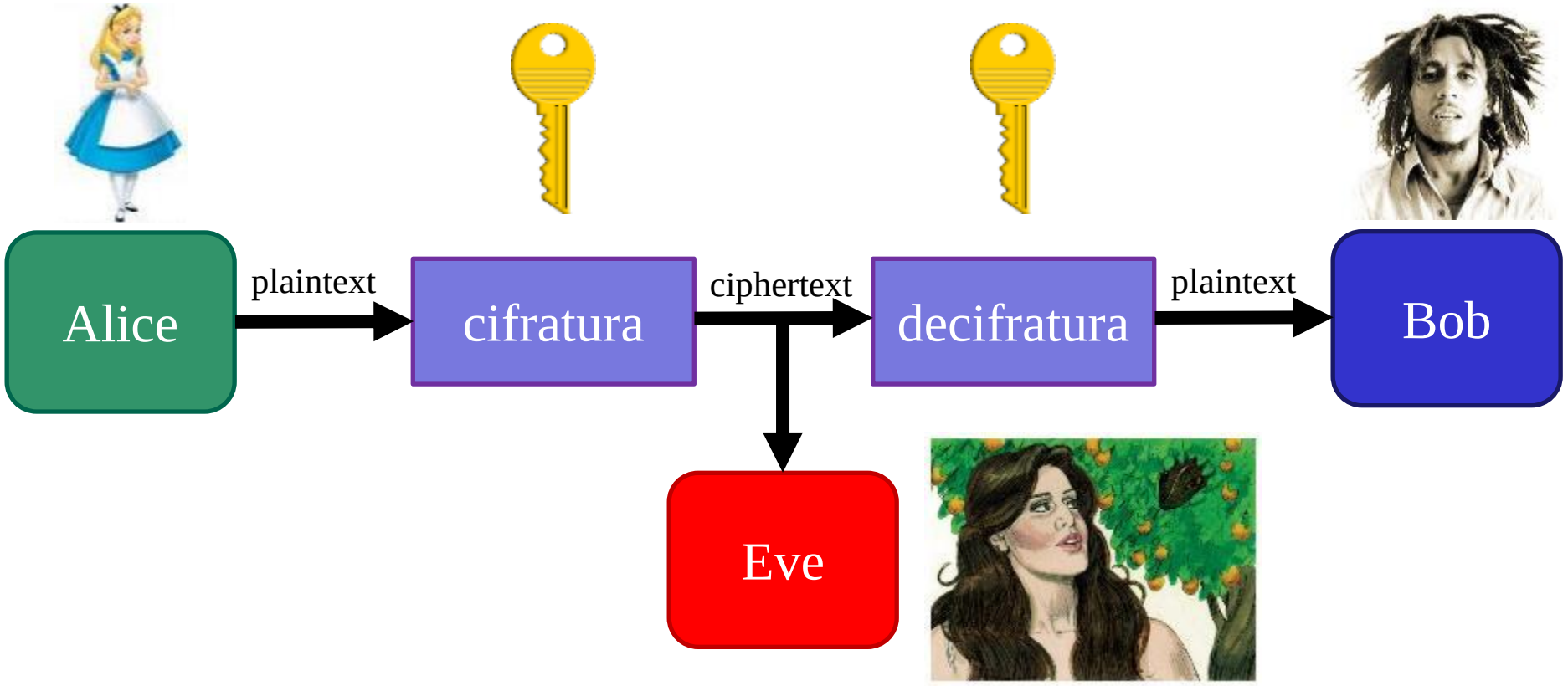
Introduzione alla crittografia

Crittologia, Crittografia, Crittanalisi

- **Crittologia**
  - Studia la comunicazione su canali non sicuri e i relativi problemi
- **Crittografia**
  - Riguarda la progettazione di sistemi sicuri
- **Crittanalisi**
  - Tratta le tecniche per “rompere” i sistemi ritenuti sicuri

Crittografia



- plaintext = testo in chiaro
- ciphertext = testo cifrato (o nascosto)
- Eva conosce il metodo di cifratura
- La segretezza del messaggio dipende dalla **chiave**

Scopi di Eve

1. Leggere il messaggio

2. Trovare la chiave e quindi leggere tutti i messaggi cifrati con quella chiave

3. Modificare il messaggio di Alice in un altro messaggio

4. Fingersi Alice

(1) e (2) sono attacchi **passivi**
(3) e (4) sono attacchi **attivi**

Oscar → Eve
Mallory → Eve

Possibili attacchi

1. **Ciphertext only:** Eva ha a disposizione solo una copia del testo cifrato

2. **Known plaintext:** Eva ha una copia del testo cifrato e del corrispondente testo in chiaro

3. **Chosen plaintext:** Eva ha temporaneamente accesso alla macchina cifrante

4. **Chosen ciphertext:** Eva ha temporaneamente accesso alla macchina decifratrice

Principio di Kerckoffs (1883)

La sicurezza di un sistema crittografico non può essere basata sulla segretezza dell'algoritmo adottato; viceversa, essa si basa sulla sicurezza della chiave.

Regole di Kerckoffs

1. Un sistema crittografico deve essere fisicamente, se non matematicamente, indecifrabile (cifrario perfetto).
2. Il sistema non deve richiedere segretezza e deve poter cadere in mani nemiche senza inconvenienti.
3. Deve essere possibile scambiare e memorizzare la chiave senza bisogno di note scritte e deve essere possibile cambiare la chiave quando gli utenti lo desiderano.
4. Il sistema deve essere applicabile alla corrispondenza telegrafica.
5. Il sistema deve essere portatile e il suo utilizzo e funzionamento non deve richiedere la disponibilità di un gran numero di persone.
6. Infine, date le circostanze in cui presumibilmente verrà utilizzato, il sistema non deve richiedere la conoscenza di una lunga serie di regole o essere difficile da applicare.

I cifrari classici

Cifrari classici

- Testo in chiaro scritto in lettere minuscole
- Testo cifrato scritto in lettere maiuscole
- Ad ogni lettera dell'alfabeto è assegnato un numero

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

- Gli spazi e la punteggiatura sono omessi

Trasposizioni e Permutazioni

- Una trasformazione che inverte l'ordine di due elementi di un insieme tenendo fissi tutti gli altri è chiamata **trasposizione**.

- Qualsiasi trasformazione uno-a-uno di un insieme di elementi ordinati su se stesso è chiamata **permutazione** di elementi dell'insieme.

- Ogni permutazione di elementi ordinati può essere espressa come sequenza di trasposizioni.

Cifrari a trasposizione

- La **scitala** è un esempio di cifrario a trasposizione: le lettere del messaggio vengono scritte per colonne anziché per righe.
- In generale, una cifratura a trasposizione è un anagramma del testo in chiaro.
- Il numero di anagrammi concepibili diventa rapidamente molto elevato. Es.: 30 lettere $\rightarrow$ 30! anagrammi diversi.
- La trasposizione non può che avvenire secondo un criterio prefissato e questo rende il sistema vulnerabile, anche per l'inconveniente, che spesso comporta, di richiedere una chiave materiale.

Cifrari a scorrimento (Cifrario di Cesare)

- Ogni lettera viene fatta scorrere in avanti di un numero segreto di posizioni

- Si sceglie come chiave un intero κ: $0 \leq \kappa \leq 25$

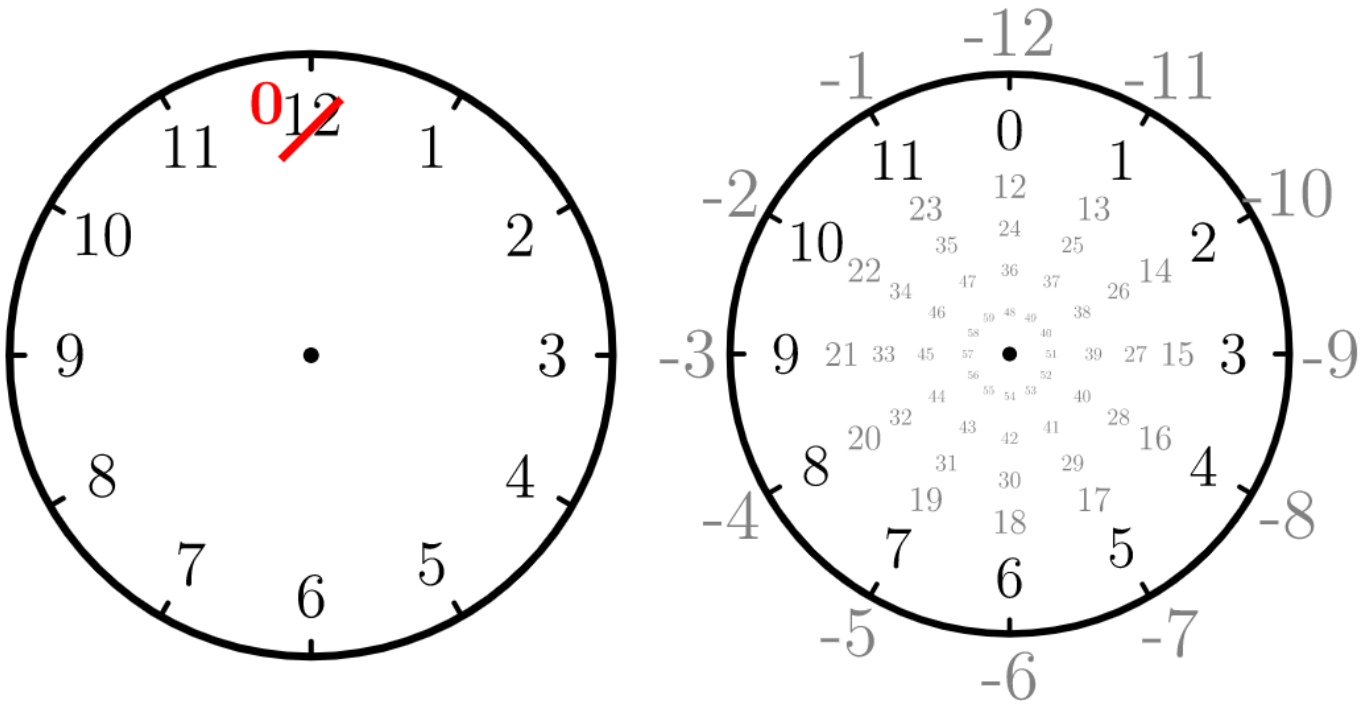
  Cifratura: $x \rightarrow x + \kappa \pmod{26}$
  Decifratura: $x \rightarrow x - \kappa \pmod{26}$

Esempio: $\kappa = 3$ $\quad gaul\ is\ divided\ into\ three\ parts$

$$JDXOLVGLYLGHGLQWRWKUHHSDUWV$$

Aritmetica modulare

Operazioni sull'orologio = Operazioni aritmetiche modulo 12



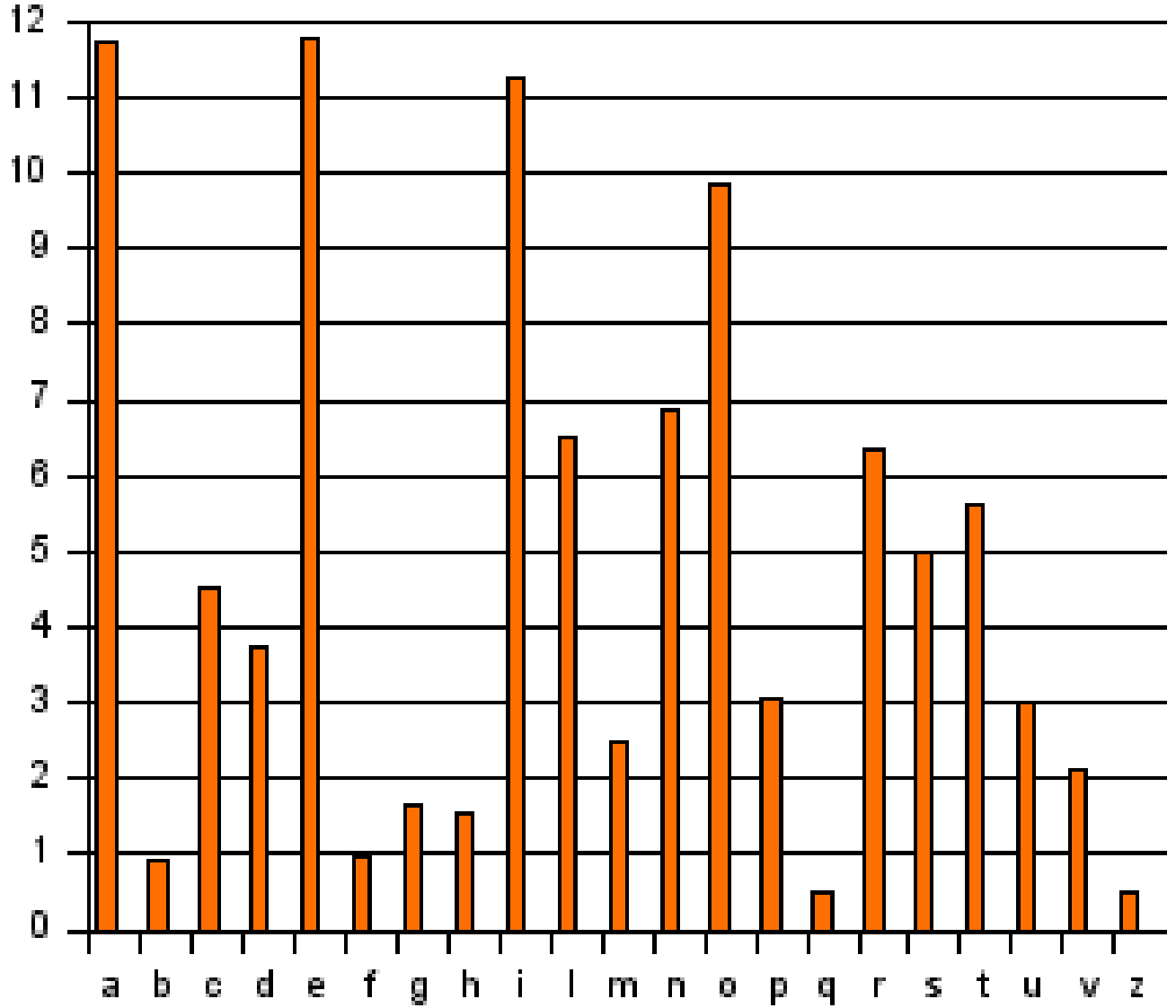
Attacchi al cifrario a scorrimento (I)

Solo testo cifrato

Strategia migliore: ricerca esaustiva (solo 26 chiavi possibili)

- Se il messaggio non si riduce a poche lettere, è improbabile che ci sia più di un messaggio di senso compiuto che possa essere il testo in chiaro
- Se il messaggio è sufficientemente lungo, un altro possibile attacco consiste nel contare la **frequenza** delle varie lettere
  - **Esempio**:
    La lettera e è la più frequente nella maggioranza dei testi italiani. Se la lettera L compare più di frequente nel testo cifrato, allora essendo e = 4 ed L = 11, una congettura ragionevole è $\kappa = 11 - 4 = 7$

Frequenze delle lettere nei testi italiani



Analisi delle frequenze

Tecnica introdotta da **Abu** Yousuf Yaqub Ibn Ishaq **Al Kindi**, uno scienziato che ha operato a Baghdad nel IX secolo. Filosofo, matematico, fisico, astronomo e esperto in musica, Al Kindi ha prodotto più di 200 libri di cui molti furono tradotti in latino nel Medio Evo.

Attacchi al cifrario a scorrimento (II)

Testo in chiaro noto

Se si conosce una lettera del testo in chiaro e la corrispondente lettera nel testo cifrato, allora si può dedurre immediatamente la chiave

Esempio:
Si sa che t (= 19) viene cifrata in D (= 3).
Allora la chiave è $\kappa = 3 - 19 = -16 = 10 \pmod{26}$

Attacchi al cifrario a scorrimento (III)

Testo in chiaro scelto

Scelta la lettera a come testo in chiaro, allora il testo cifrato fornisce la chiave

Esempio:
Se il testo cifrato è H, allora la chiave è $\kappa = 7$

Attacchi al cifrario a scorrimento (IV)

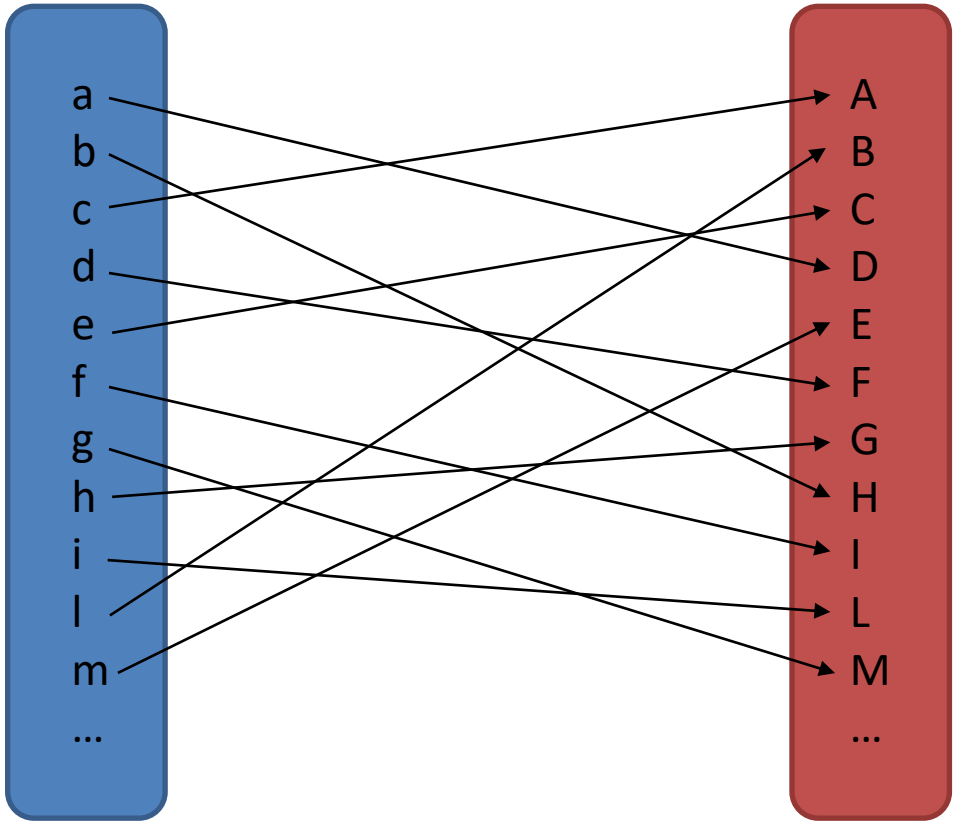
Testo cifrato scelto

Scelta la lettera A come testo cifrato, allora il testo in chiaro è l'opposto della chiave

Esempio:
Se il testo in chiaro è h, allora la chiave è $\kappa = -7 = 19 \pmod{26}$

Cifrari monoalfabetici

- Molti cifrari classici sono **monoalfabetici**, ovvero creano una mappatura fissa tra ciascuna lettera in chiaro e la corrispondente lettera cifrata.



Evoluzione dei cifrari (simmetrici)

- Leon Battista Alberti, Vigenère, Hill, Playfair… Enigma

Cifrari a blocco

- In molti sistemi crittografici precedenti, la modifica di una lettera nel del testo in chiaro cambia esattamente una lettera nel testo cifrato.
- In questo modo gli attacchi basati sull'analisi delle frequenze sono molto semplici.
- I cifrari a blocchi possono evitare questi problemi criptando simultaneamente blocchi di molte lettere o numeri.