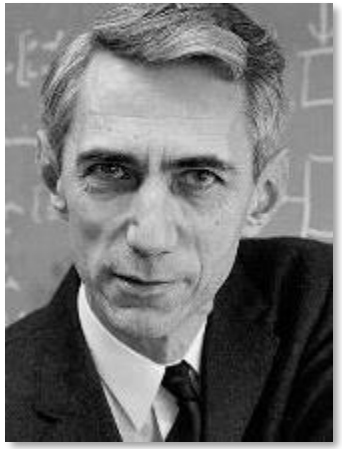
Il cifrario perfetto

Cifrario perfetto (Shannon 1949)

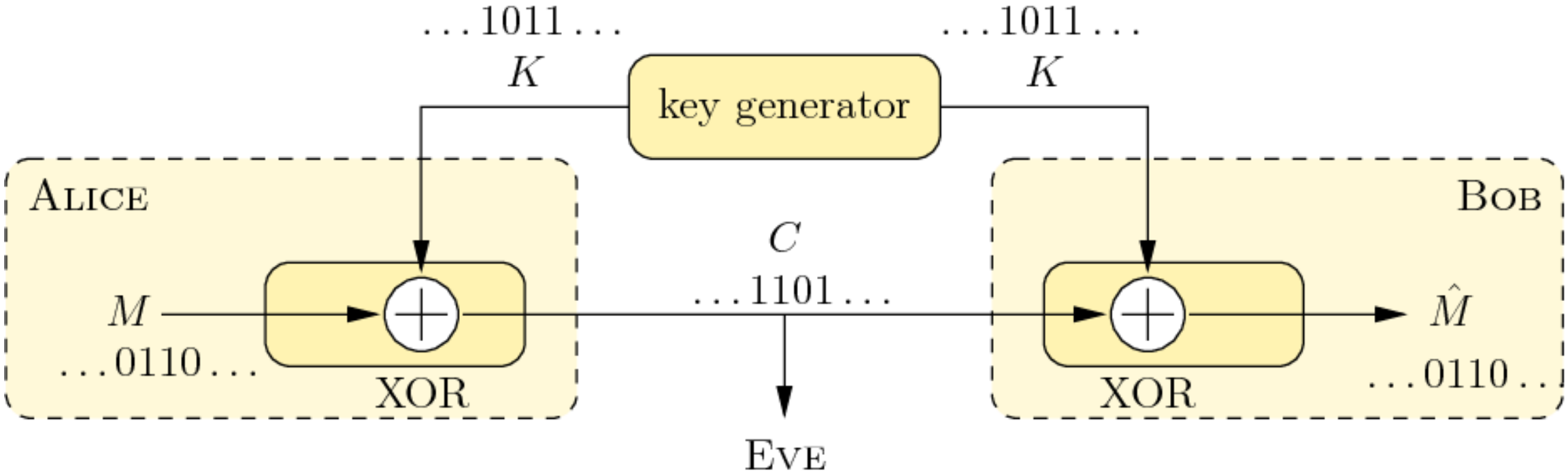


- Matematicamente inviolabile
- La sua inviolabilità non è dovuta ad alcuna limitazione delle capacità di calcolo degli avversari.
  - La chiave è lunga (almeno) come il testo in chiaro
  - La chiave è generata randomicamente
  - La chiave si usa una sola volta

ONE TIME PAD (G. Vernam, J. Mauborgne ≈ 1918)

- Si può provare matematicamente la sua sicurezza
- Il testo cifrato ha la stessa lunghezza del testo in chiaro

One-Time pad


...1011...
K
key generator
...1011...
K
Alice
Bob
C
...1101...
M
...0110...
XOR
XOR
M̂
...0110..
Eve

Inviolabilità del one-time pad

(plaintext)	00101001
(key) +	10101100
(ciphertext)	10000101

➢ Analogamente alla versione binaria (sopra), può essere formulata con lettere. La chiave è quindi un insieme casuale di caratteri tra 0 e 25. La decodifica utilizza la stessa chiave, ma con valori opposti.

➢ **Ciphertext-only attack**: non ha successo

Esempio: FIOWPSLQNTISJQL

potrebbe provenire, con la stessa probabilità da

wewillwinthewar o da

theduckwantsout così come ogni altro messaggio di quella lunghezza

➢ Questo perché gli scorrimenti delle lettere sono tutti ugualmente probabili.

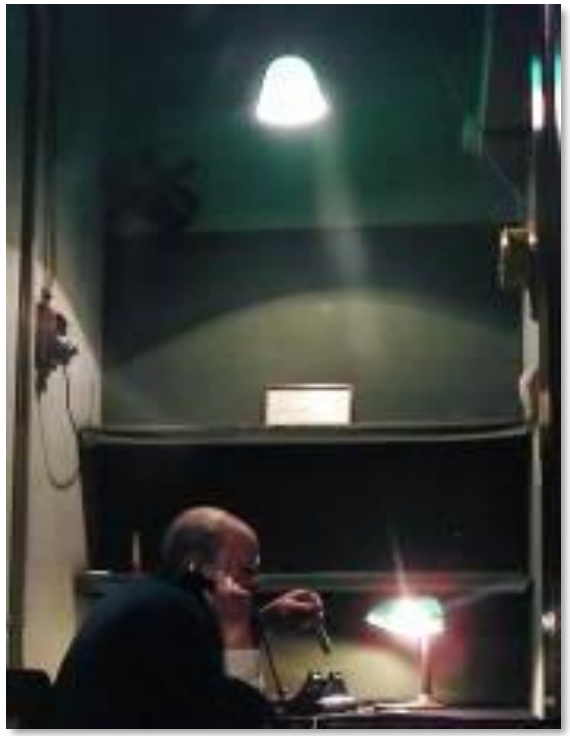
Inviolabilità del one-time pad

- **Known-plaintext attack**: Se si dispone di un pezzo di testo in chiaro, è possibile trovare il pezzo corrispondente della chiave, ma nulla si può dire sul resto della chiave.

- **Chosen-plaintext or chosen-ciphertext attack**: Si può anche pensare di trovare parti di chiave o addirittura l'intera chiave, ma il risultato è inutile, poiché le parti di chiave scoperte non saranno più utilizzate.

One-time pad in pratica

- Una versione pratica dell'OTP è stata utilizzata per la linea telefonica **POTUS-PRIME** tra Winston Churchill e Franklin Delano Roosevelt durante la Seconda Guerra Mondiale.
- Il flusso era memorizzato su grandi dischi fonografici in gommalacca contenenti rumore casuale.
- Il segnale vocale dell'oratore veniva moltiplicato per questo rumore e trasmesso attraverso l'oceano.
- All'altra estremità, il segnale ricevuto veniva moltiplicato per lo stesso rumore, fornito da una registrazione identica e accuratamente sincronizzata.



Problemi pratici del cifrario perfetto

- Alice e Bob devono generare una nuova chiave ogni volta che è necessario trasmettere un nuovo messaggio
- È necessaria un'enorme quantità di bit nella chiave, e devono essere casuali
- Il One-time pad non è utilizzabile per le comunicazioni quotidiane
- Alternativa: rinunciare alla segretezza perfetta e utilizzare un cifrario con una chiave più corta del messaggio
- Collegare la sicurezza alla soluzione di un problema difficile, possibilmente nella classe di problemi NP (tempo polinomiale non deterministico)