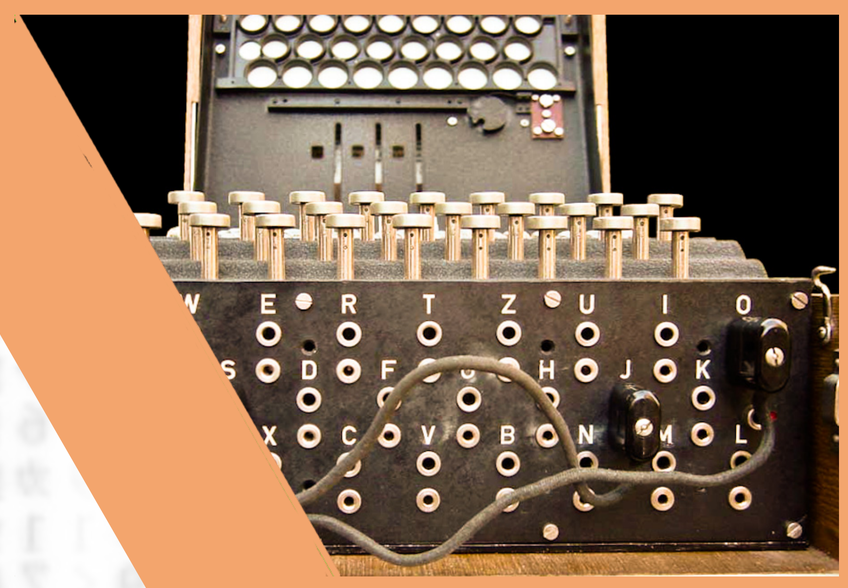
Università degli Studi di Ferrara
- EX LABORE FRUCTUS -

UniFestival

Trasmissione dei dati

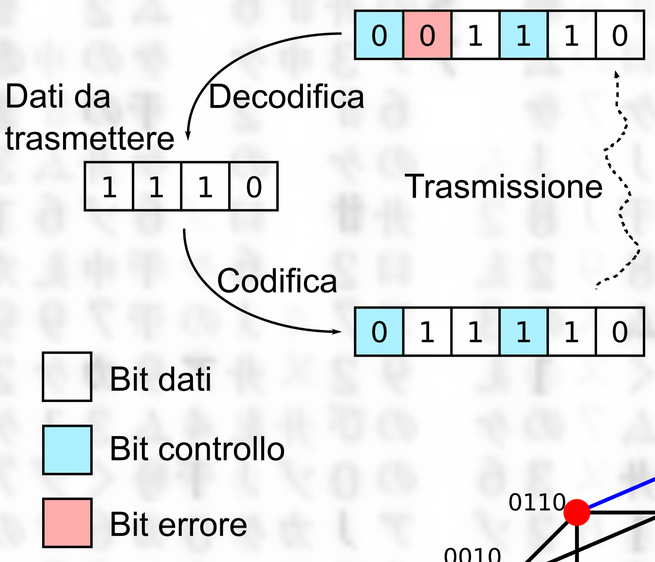


La crittografia cifra i messaggi per renderli illeggibili a chi non è un autorizzato. Un esempio è la macchina Enigma usata dai tedeschi nel corso della seconda guerra mondiale.

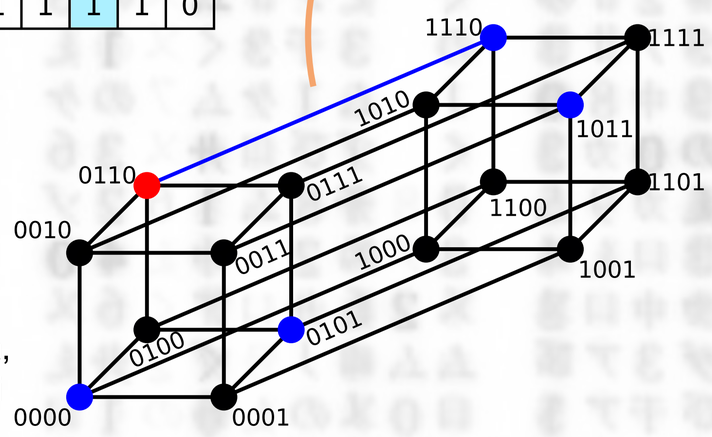
Quando si trasmettono dei dati emergono due esigenze:
correggere gli errori che avvengono durante la trasmissione e nascondere il contenuto a chi non è autorizzato a vederlo.

Correzione degli errori

Teoria dei Codici

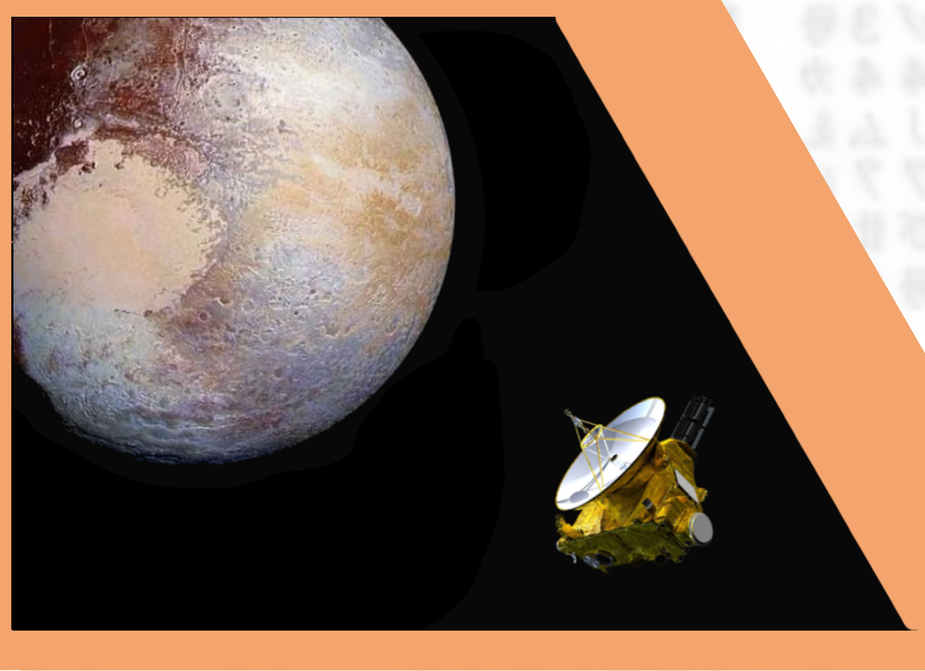


Codice autocorrettivo: i dati da trasmettere vengono codificati e, con la decodifica, vengono corretti gli eventuali errori avvenuti durante la trasmissione



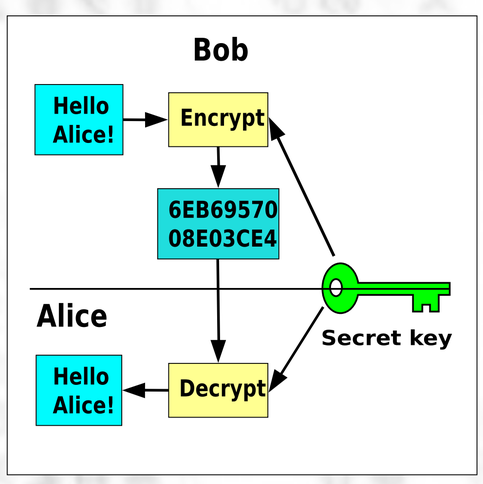
Distanza tra le parole del codice: la parola ricevuta (in rosso) viene corretta con la parola più vicina tra quelle del codice (in blu)

I codici autocorettivi vengono usati per correggere gli errori di trasmissione in tutte le comunicazioni elettroniche. Per esempio, trasmissioni satellitari, telefoniche, scrittura dati su cd, dvd e hard-disk, eccetera

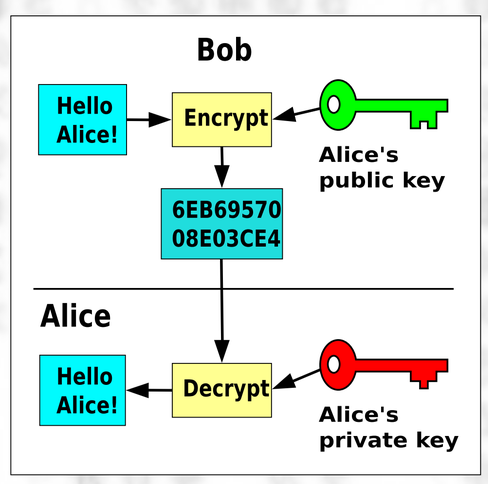


Privacy

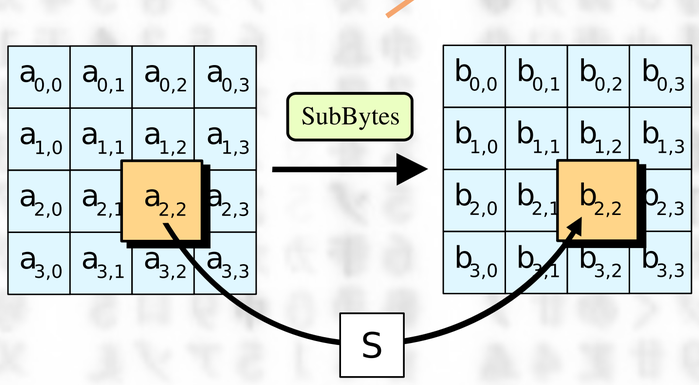
Crittografia



I cifrari a chiave privata usano la stessa chiave sia per cifrare che per decifrare



I cifrari a chiave pubblica usano due chiavi diverse: una per cifrare ed una per decifrare



Il cifrario AES è uno dei cifrari a chiave privata più diffusi.
Esso agisce sostituendo i byte di un messaggio usando l'aritmetica dei campi finiti

$$a^{\varphi(n)} \equiv 1 \ (n)$$

Il cifrario RSA è uno dei primi e più famosi cifrari a chiave pubblica.
Modifica i messaggi trattandoli come numeri e usando varie proprietà algebriche, tra cui il Teorema di Eulero.

30° Anniversario
1985-2015
Dipartimento di Matematica e Informatica
Università di Ferrara
dmi.unife.it