COESIONE ITALIA 21-27 PIEMONTE
Cofinanziato dall'Unione europea
REGIONE PIEMONTE

CODICI CORRETTORI

Sicurezza informatica

Elena Maria Dal Santo

elenamaria.dalsanto@its-ictpiemonte.it

Intervento realizzato da
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

La SICUREZZA INFORMATICA

È

L’insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici (di un’azienda)

Serve a

Garantire la triade

Confidentiality

Integrity

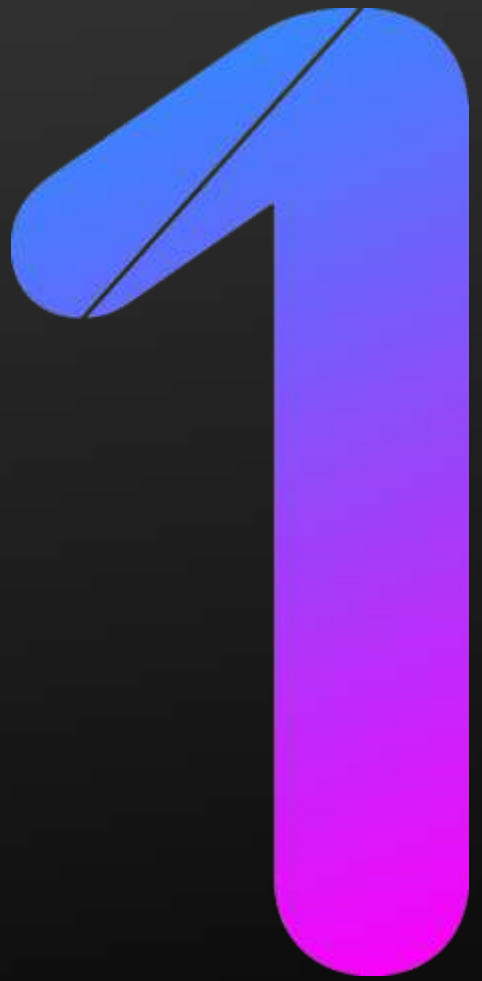
Availability

Fino ad adesso i nostri problemi erano causati da un attaccante esterno. Per difenderci, abbiamo visto vari modi di difenderci, costruendo codici e canali sicuri…

E se il problema fosse proprio il CANALE?

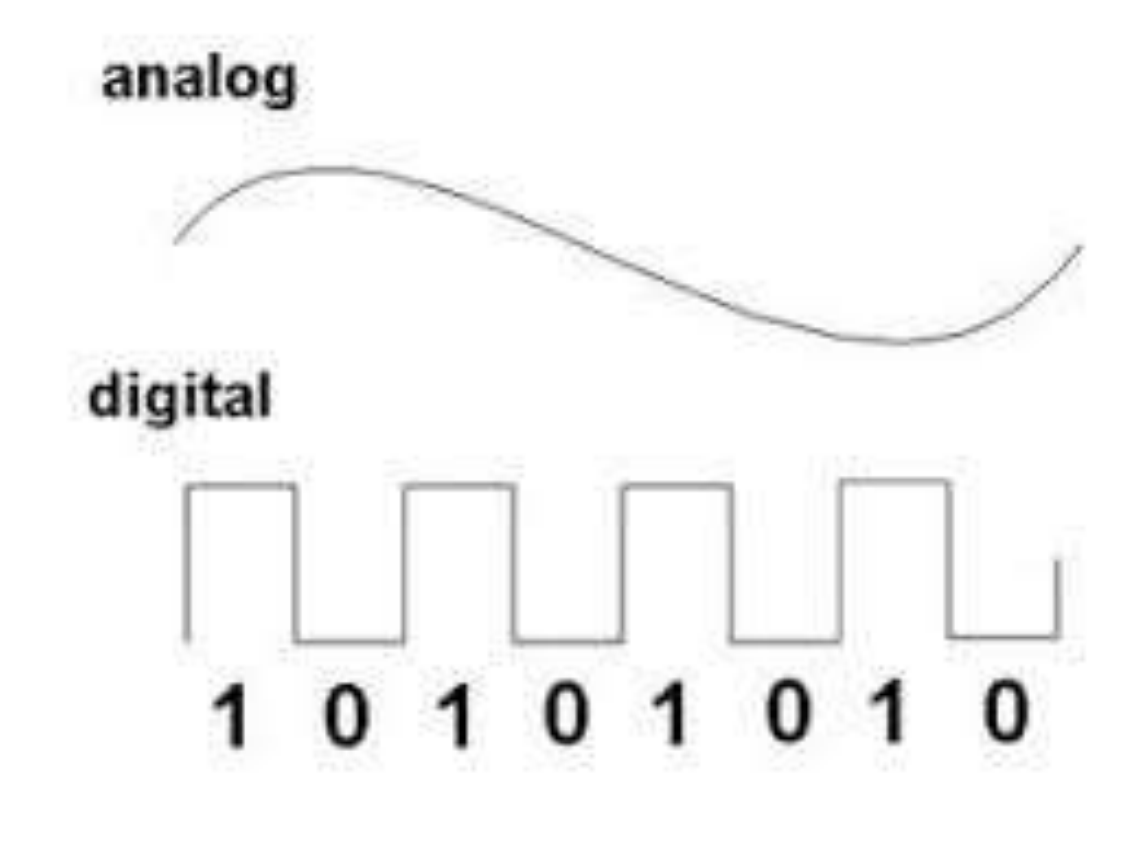
Integrità


Mi hanno messo in punizione
Ascolta una canzone
Ha creato una pozione
Ho fatto colazione
È ancora in circolazione



Trasmissione su canale

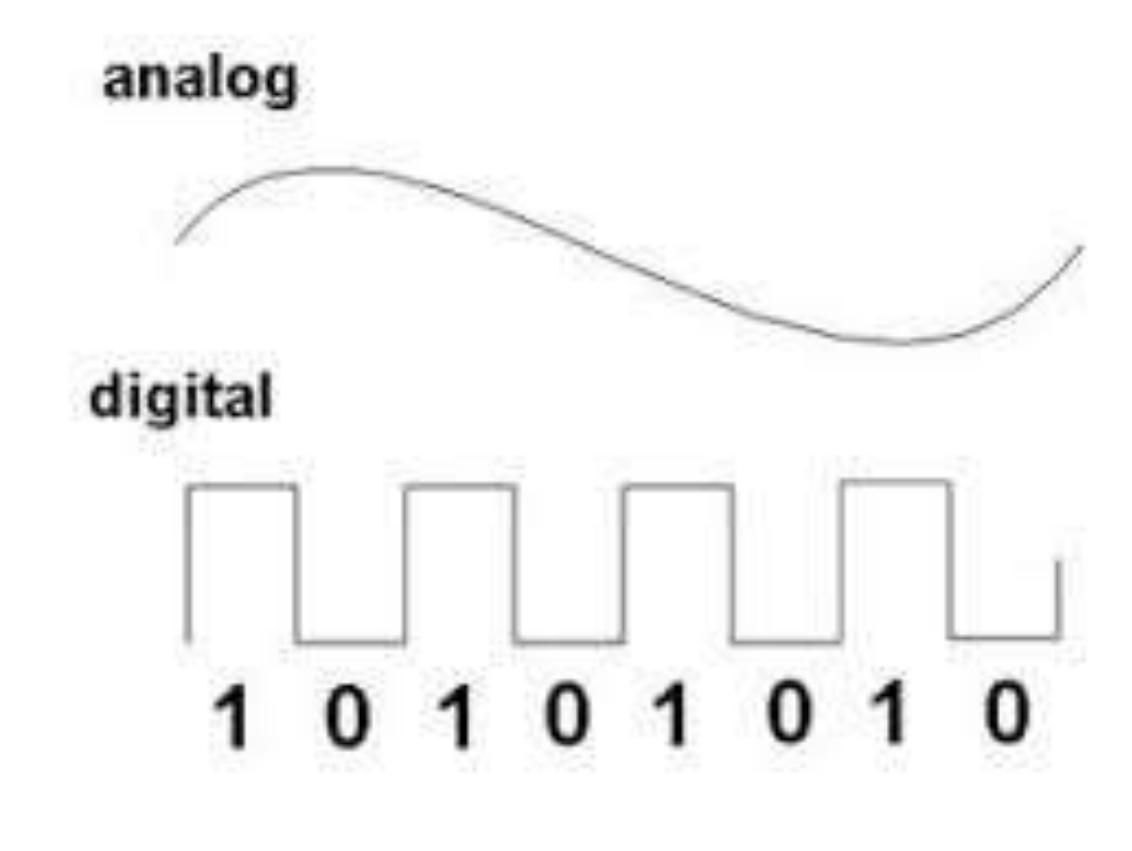
Trasmissione su canale



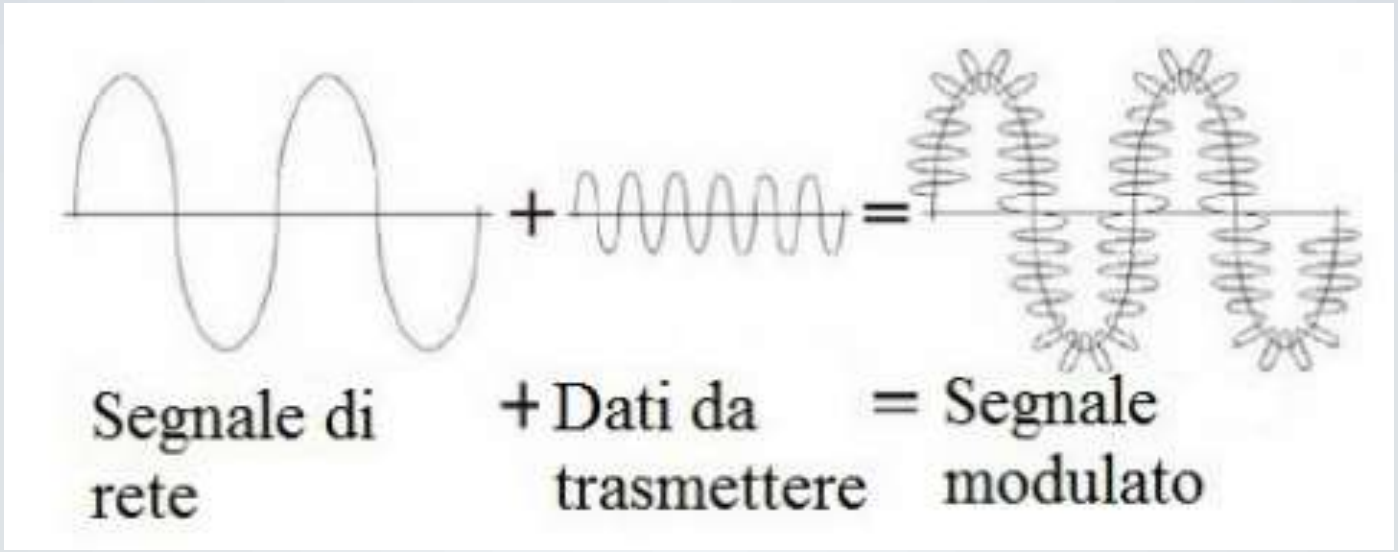
Iniziamo facendoci un'idea dei due diversi tipi di segnali più comunemente usati e visualizziamoli in modo semplice.

Come si vede dalla figura, il segnale analogico è continuo nel tempo, mentre i segnali digitali sono temporalmente distinti (ricordano il codice Morse).

Trasmissione su canale



Il segnale digitale è solitamente più ‘’immune’’ a problemi di trasmissione, perciò per questa lezione di concentreremo sul segnale analogico.



Quando si parla di trasmissione di dati su un canale (rete), l'idea è che l'insieme di dati da trasmettere viene innestato direttamente sulla rete, che si occupa quindi di trasportarlo da mittente a destinatario.

Questo tipo di comunicazione è usato nelle applicazioni più svariate, che vanno dalla mobilità (treni) alla ricerca, e sfruttano ampiamente l'infrastruttura della rete elettrica.

L'idea di inviare messaggi attraverso una rete già esistente ed estesa come quella elettrica non è da sottovalutare...

Pro:

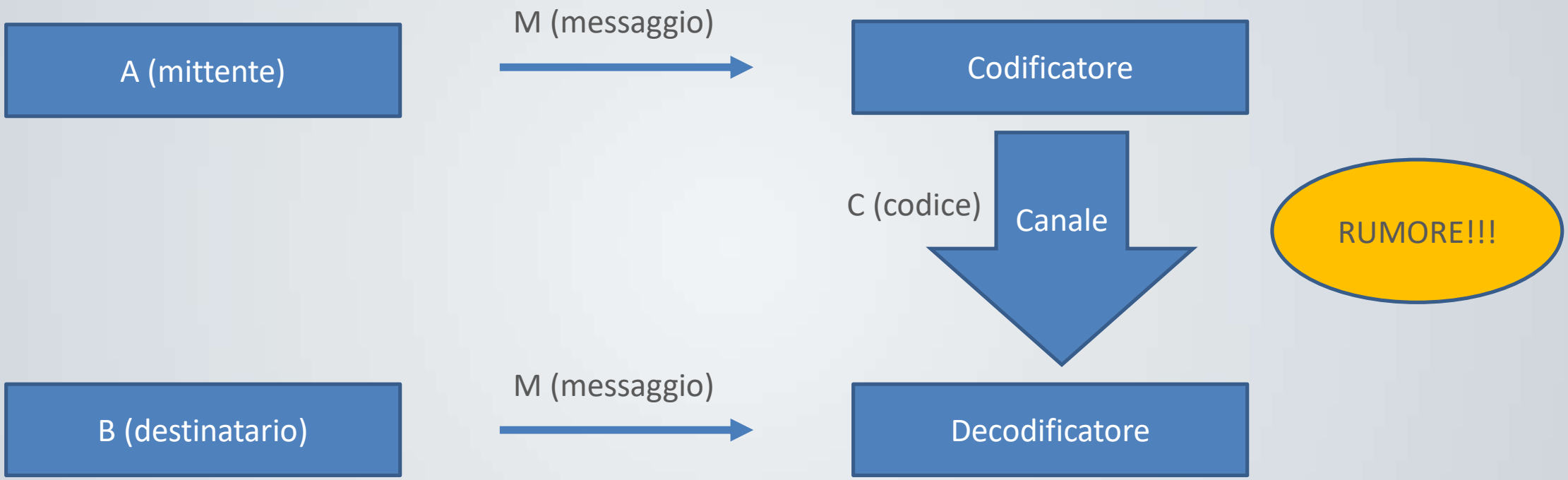
1. Esiste già

2. Ampiamente diffusa: le comunicazioni potrebbero arrivare anche in aree dove, ad esempio, la rete internet non è disponibile

Contro:

1. I cavi elettrici sono molto esposti a intemperie

2. In caso di blackout, tutte le comunicazioni andrebbero perdute


A (mittente)
M (messaggio)
Codificatore
C (codice)
Canale
RUMORE!!!
B (destinatario)
M (messaggio)
Decodificatore

I codici correttori

I codici correttori servono proprio a rilevare e correggere questo disturbo ed eventuali errori che potrebbe aver provocato.

1) Come posso RILEVARE un errore?

2) Come posso CORREGGERE un errore?

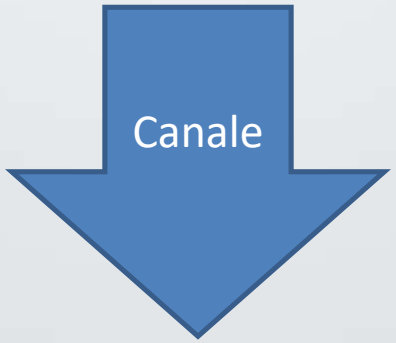
3) Esiste un modo infallibile e certo per rilevare e correggere un errore?

Una prima idea…

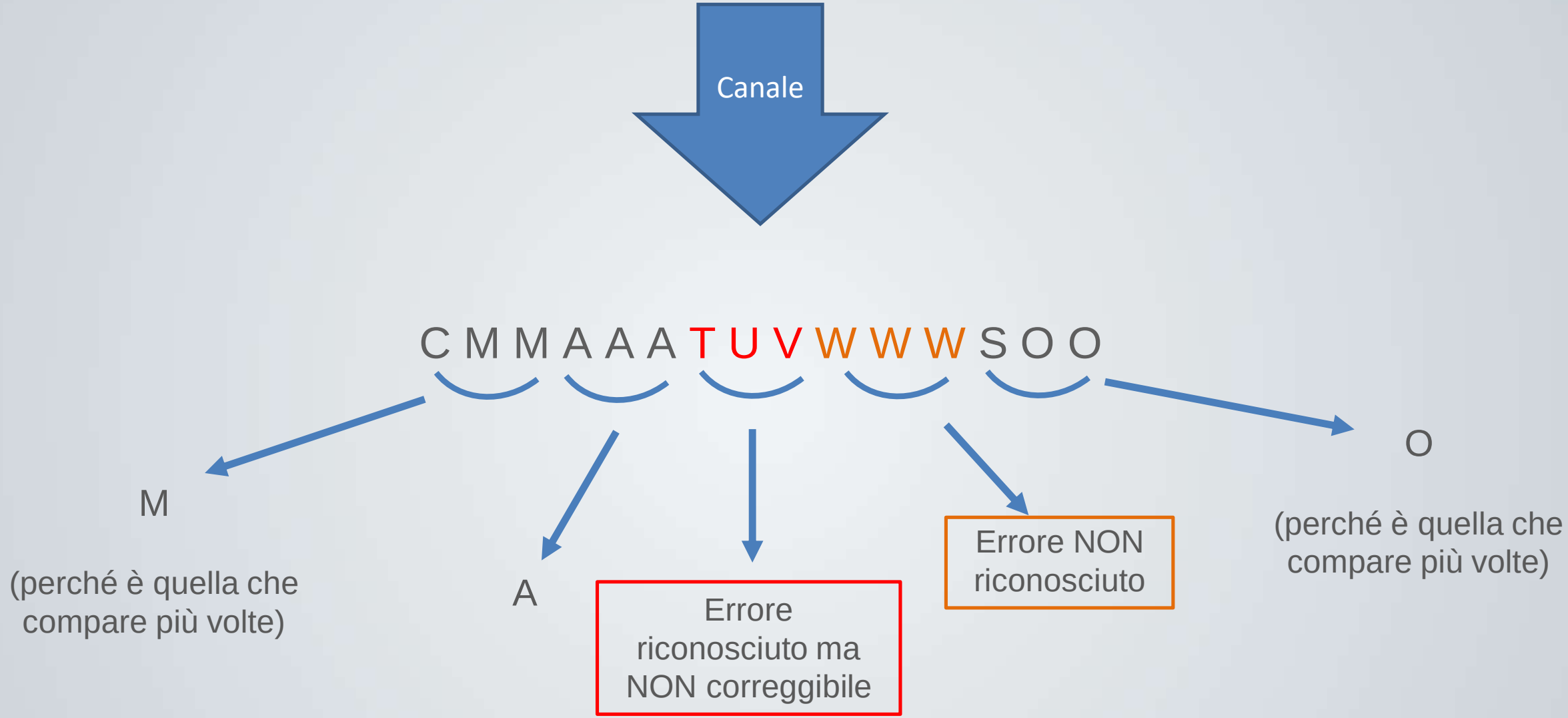
Il metodo della RIDONDANZA

Voglio inviare la parola ‘’ MATTO ‘’ ma scrivo

M M M A A A T T T T T T O O O



I caratteri ‘’in più’’ vengono detti caratteri DI CONTROLLO


Canale
C M M A A A T U V W W W S O O
M
(perché è quella che compare più volte)
A
Errore riconosciuto ma NON correggibile
Errore NON riconosciuto
O
(perché è quella che compare più volte)

Il numero di caratteri diversi tra due parole (quella attesa e quella ottenuta) di chiama distanza di Hamming.

Es. la distanza di Hamming tra ‘’dire’’ e ‘’fare’’ è 2.

Se tra tutte le distanze di Hamming prendiamo quella più piccola, questa sarà la distanza minima tra le parole. Per comodità, la indicheremo con la lettera *d.*

Fondamentalmente è il numero minimo di caratteri che devono cambiare per considerare due parole ‘’diverse’’

Nella nostra lingua, ovviamente, questa distanza è pari a 1

Es. le parole ‘’gelato’’ e ‘’velato’’

Perché ci interessa?

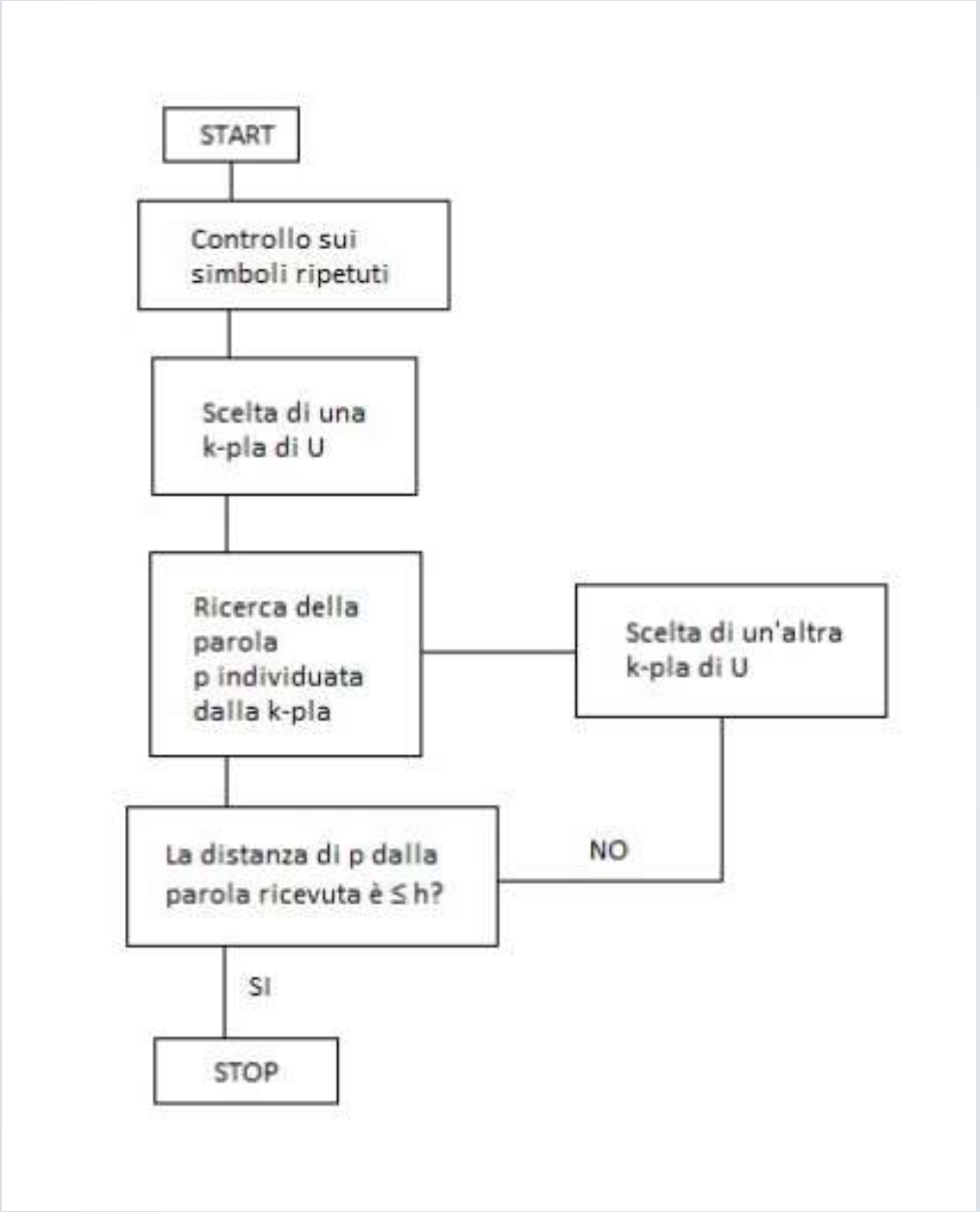
Da questa distanza minima dipende la capacità di un codice di rilevare e correggere errori.

Un codice è un grado di RILEVARE

$$d-1 \text{ errori}$$

Un codice è in grado di CORREGGERE

$$\frac{d-1}{2} \text{ errori}$$


START
Controllo sui simboli ripetuti
Scelta di una k-pla di U
Ricerca della parola p individuata dalla k-pla
Scelta di un'altra k-pla di U
La distanza di p dalla parola ricevuta è ≤ h?
NO
SI
STOP

I codici vengono costruiti in modo da poter correggere più o meno errori, a seconda delle necessità.

Ad esempio, nella RAM gli errori sono molto rari (è grave averne anche solo uno!) perciò un codice che sia in grado di rilevare e correggere anche solo un errore va più che bene.

Nel campo delle comunicazioni, invece, si possono avere molte sorgenti di rumore e molti disturbi, poter rilevare e correggere un solo errore non è sufficiente.

Perché ci interessa?

Un codice è un grado di RILEVARE

d-1 errori

Un codice è in grado di CORREGGERE

$$\frac{d-1}{2} \text{ errori}$$

Questo però significa che in un linguaggio come il nostro, il verificarsi di un errore è un fatto piuttosto grave.

Basta infatti un solo carattere per distinguere le parole nella nostra lingua, perciò d = 1

Ciò significa che possiamo rilevare e correggere 0 errori!!!

Serve un altro metodo di controllo…

Il codice fiscale

Come possiamo fidarci a prescindere del fatto che il codice fiscale di una persona sia effettivamente corretto? Se una persona ve l'ha comunicato al telefono, le probabilità che la comunicazione sia stata disturbata da eventuali rumori sono molto alte!

→ l'ultima lettera del codice fiscale è un carattere di controllo, ovvero un carattere non associato direttamente alla vostra identità, ma ottenuto tramite calcoli sulla base dei caratteri che lo precedono.

Il codice fiscale

Il codice fiscale

6 caratteri alfabetici, 3 per il cognome e 3 per il nome

Il codice fiscale

Anno di nascita e mese di nascita, a cui viene associata una lettera in base a una tabella

Il codice fiscale

Anno di nascita
Mese di nascita, a cui viene associata una lettera in base a una tabella
Giorno di nascita

Il codice fiscale

Il codice fiscale

Tabella C – conversione dei caratteri con posizione di ordine pari				
A o 0 = 0	F o 5 = 5	K = 10	P = 15	U = 20
B o 1 = 1	G o 6 = 6	L = 11	Q = 16	V = 21
C o 2 = 2	H o 7 = 7	M = 12	R = 17	W = 22
D o 3 = 3	I o 8 = 8	N = 13	S = 18	X = 23
E o 4 = 4	J o 9 = 9	O = 14	T = 19	Y = 24
				Z = 25

Per gli otto caratteri con posizione di ordine dispari:

Tabella D– conversione dei caratteri con posizione di ordine dispari				
A o 0 = 1	F o 5 = 13	K = 2	P = 3	U = 16
B o 1 = 0	G o 6 = 15	L = 4	Q = 6	V = 10
C o 2 = 5	H o 7 = 17	M = 18	R = 8	W = 22
D o 3 = 7	I o 8 = 19	N = 20	S = 12	X = 25
E o 4 = 9	J o 9 = 21	O = 11	T = 14	Y = 24
				Z = 23

RSSMRA80A01H501U

8|18|12|12|8|0|19|0|1|0|7|13|0|0

Il codice fiscale

Tabella E – determinazione del "check-digit"				
0 = A	5 = F	10 = K	15 = P	20 = U
1 = B	6 = G	11 = L	16 = Q	21 = V
2 = C	7 = H	12 = M	17 = R	22 = W
3 = D	8 = I	13 = N	18 = S	23 = X
4 = E	9 = J	14 = O	19 = T	24 = Y
				25 = Z

La somma dei numeri trovati è 98

98 = 26 x 3 + 20

Si ma… quindi?

Tutto questo per dire che se ci fosse anche solo un errore nella trasmissione del codice fiscale, noi potremmo non accorgercene, ma ‘’i conti’’ non tornerebbero, perché il carattere di controllo non coinciderebbe con quello atteso.

Il carattere di controllo permette di RILEVARE in modo sicuro un errore quando si verifica.

Allo stesso modo funzionano i codici ISBN e i codici a barre.