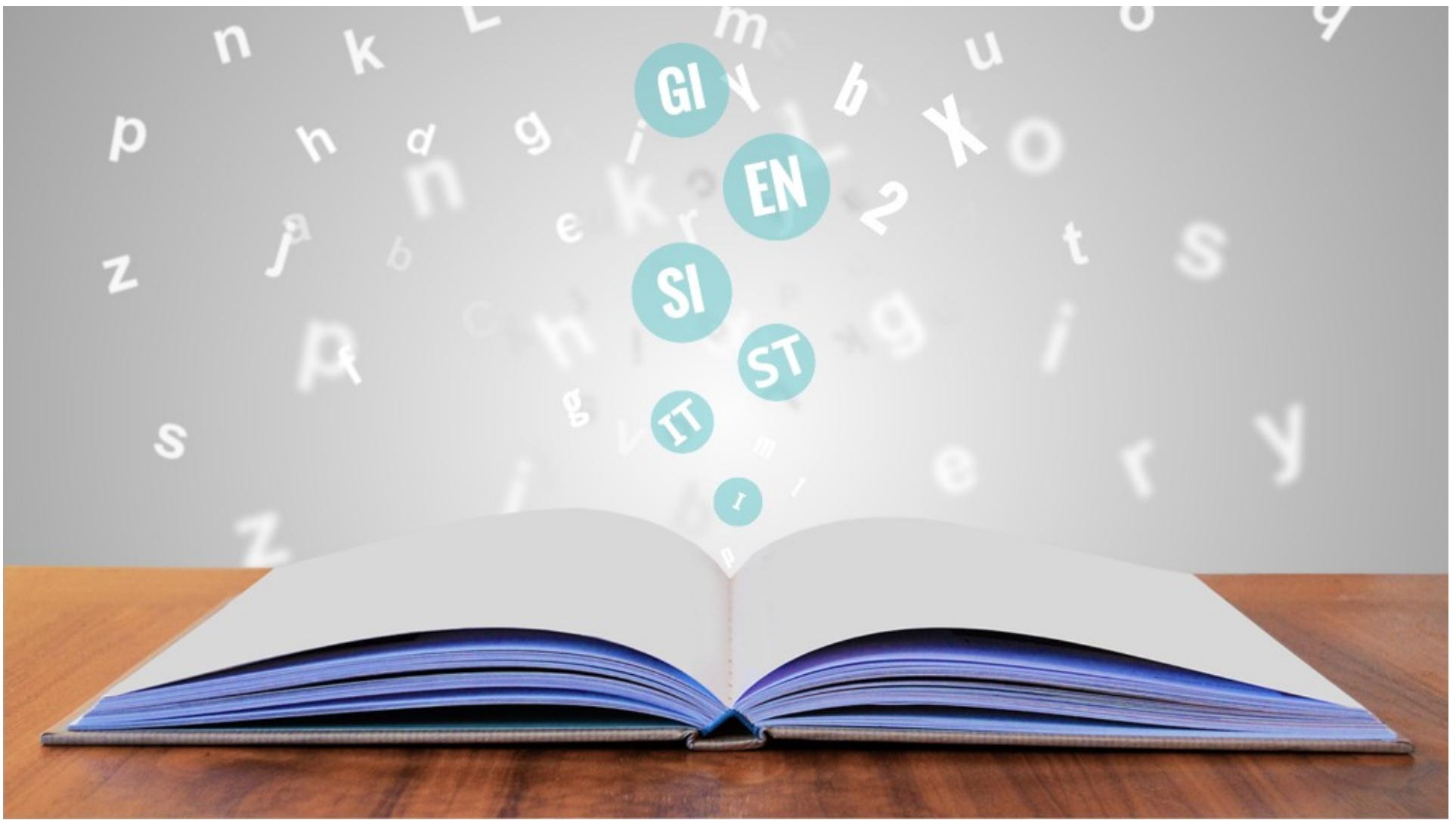


# Percorso Maturità

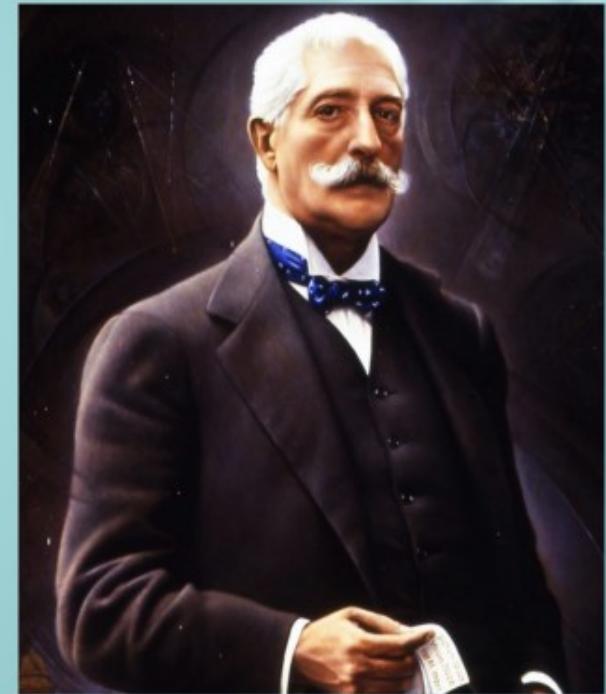


A cura di  
Alessandro Catalano  
V C INF



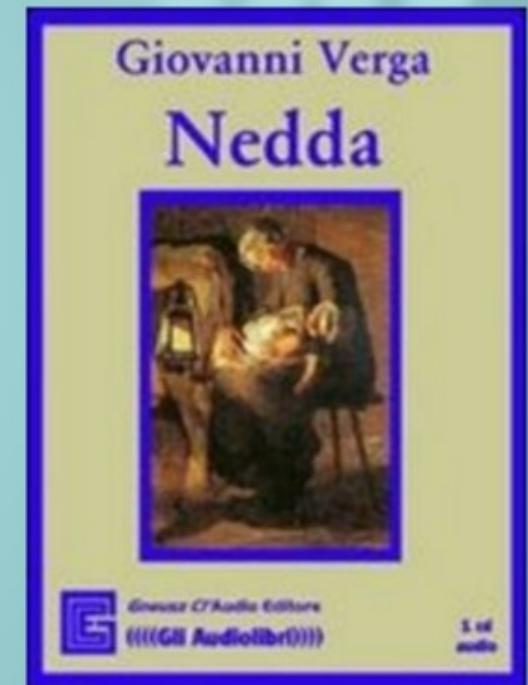
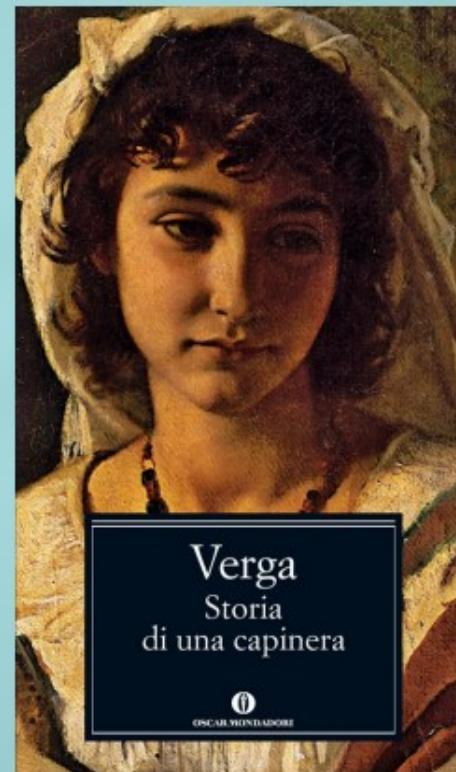
# Giovanni Verga

Giovanni Verga nasce a Catania il 2 settembre 1840 da una famiglia nobile di piccoli proprietari terrieri. Politicamente è stato un conservatore-nazionalista e interventista durante la prima guerra mondiale



# I primi anni e il preverismo

Non si interessò molto ai classici della letteratura e preferì gli scrittori francesi moderni. A 25 anni comincia a viaggiare per liberarsi della sua cultura ristretta alla provincia. In questi anni scrive i suoi primi romanzi di carattere romantico in cui parla principalmente degli ambienti aristocratici.



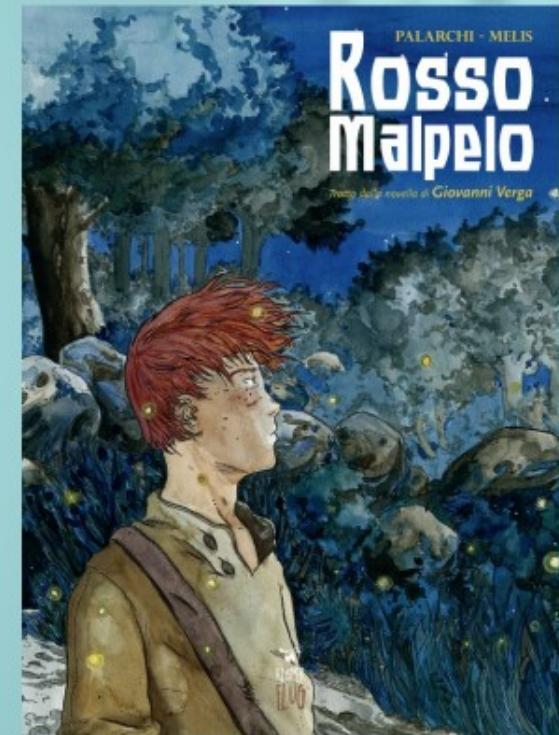
# La svolta verista - Rosso Malpelo

Nel 1878, dopo alcuni anni di crisi, avviene la svolta verista. Verga non descrive più il mondo borghese, ma il mondo umile e povero siciliano.

Le caratteristiche del verismo sono: far scomparire il narratore dall'opera e quindi narrare il romanzo in forma **impersonale** (oggettivamente) e "**l'opera deve sembrare essersi fatta da sé**".

Verga condisce le sue opere con il **pessimismo**.

La prima opera verista è stata **Rosso Malpelo** (Vita dei Campi).



# Poetica e tecnica narrativa

- L'autore deve eclissarsi e porre il lettore faccia a faccia con il fatto
- I personaggi non devono essere introdotti ma è il lettore che deve farsi un'idea su di essi durante il corso dell'opera
- Il narratore non è più lo scrittore, colto, ma un personaggio appartenente al contesto dell'opera
- Pessimismo → rifiuto democrazia
- Darwinismo sociale → i vincitori di oggi saranno i vinti di domani



# Il ciclo dei vinti - Malavoglia

Il romanzo più famoso di Verga è probabilmente I Malavoglia, pubblicato nel 1881

Due punti di vista:

- Malavoglia (nobile)
- popolo (rude e volgare)

Ideale dell'ostrica

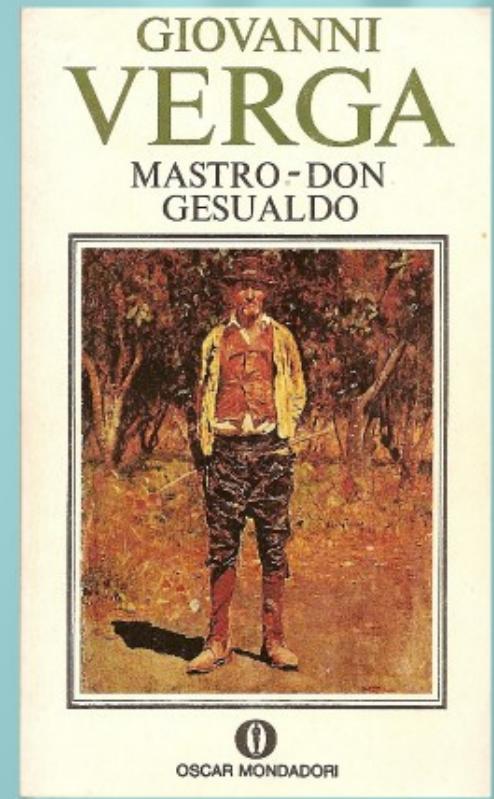


# Il ciclo dei vinti - Mastro don Gesualdo

Il romanzo, pubblicato nel 1888, narra la vicenda dell'omonimo protagonista, ed è ambientato a Vizzini, in Sicilia.

Ambiente borghese-aristocratico

Punto di vista del protagonista



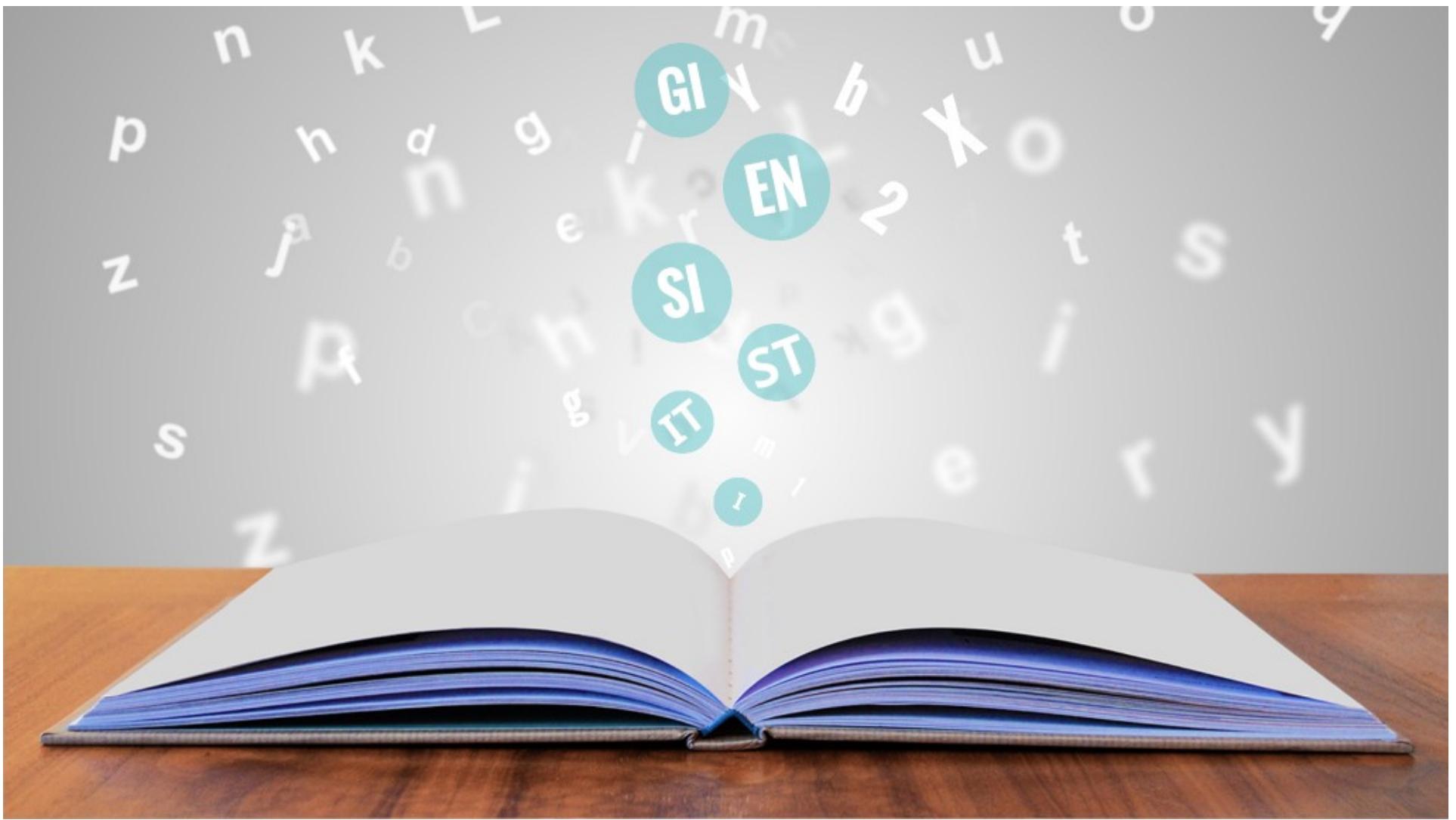
# Novelle rusticane - La roba

La novella, pubblicata nel 1883, tratta della bramosia di possesso di Mazzarò, un contadino e ricco proprietario terriero, e della sua "roba"

Duro lavoro e attaccamento ai beni materiali

L'uomo è destinato a perire quindi non si devono sacrificare gli affetti in favore della ricchezza





# Prima guerra mondiale

Chiamata anche la "Grande Guerra", è stato il primo conflitto a coinvolgere le potenze mondiali di tutto il mondo.



# Le cause

- Nazionalismo
- Competizione economica
- Gara imperialistica
- Questione d'Oriente



# La scintilla

La scintilla del conflitto fu l'assassinio dell'arciduca Francesco Ferdinando erede al trono d'Austria avvenuto il 28 giugno 1914 a Sarajevo, in Bosnia, da parte di uno studente indipendentista serbo, Gavrilo Princip.



# L'inizio della guerra

Il 23 luglio l'Austria inviò alla Serbia una nota di protesta che, seppur quest'ultima accettò, non impedì la dichiarazione di guerra avvenuta il 28 luglio. Alla dichiarazione di guerra dell'Austria alla Serbia seguì una reazione a catena:

- Russia si mobilita in difesa della Serbia
- Germania dichiara guerra a Russia, Francia e Gran Bretagna (Intesa)
- L'Impero ottomano si schierò a favore degli imperi centrali



# I fronti di guerra



Oltre a questi fronti terrestri, ci fu un altro fronte sull'oceano Atlantico.

# L'Italia in guerra

Triplice Alleanza → valore difensivo

- Neutralisti (liberali giolittiani, socialisti)
  - Interventisti (nazionalisti, giornalisti e intellettuali)

## Patto di Londra all'insaputa del Parlamento

## Garantiva all'Italia le terre irredenti



# Un nuovo tipo di guerra

- Morte di massa: 9 milioni di persone e 40 milioni di feriti
- Trincee
- Esasperazione dei soldati
- Problemi psicologici
- Nuovi armamenti: artiglieria, mitragliatrici, esplosivi ad alto potenziale e *gas tossici*.



# L'intervento degli Stati Uniti

Nel 1917 gli Stati Uniti entrarono in guerra a favore dell'Intesa per riprendere i soldi dei prestiti in favore di Francia e Gran Bretagna.

Inoltre la guerra sottomarina a oltranza dei tedeschi danneggiava i commerci attraverso l'Atlantico.



# Fine della guerra - Italia

Il 24 ottobre 1917 la pesantissima sconfitta di Caporetto dovuta all'incapacità del generale Cadorna (poi sostituito con Diaz)

La prima tappa per la fine della guerra fu la vittoria **italiana** sul fronte meridionale con l'offensiva scatenata esattamente un anno dopo la sconfitta di Caporetto e finita il 4 novembre dello stesso anno con la firma dell'armistizio.



# Fine della guerra - Germania e Imperi Centrali

Fronte orientale → vittoria imperi centrali

Disfatta di tutti gli alleati della Germania



Impero ottomano  
in Palestina e Siria



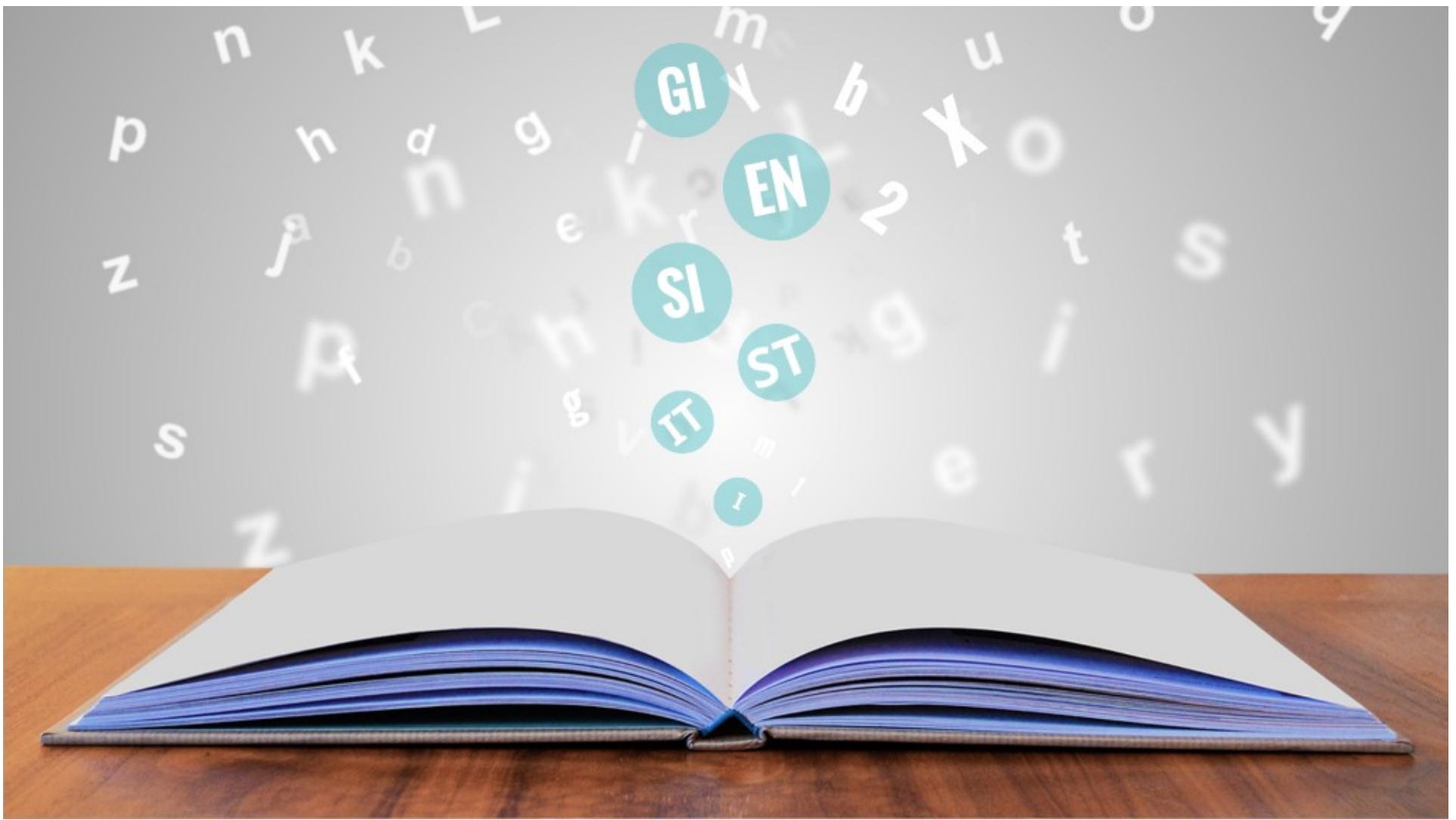
Impero asburgico per  
problemri interni

La Germania sul fronte occidentale perse  
contro l'Intesa rafforzata dagli Americani



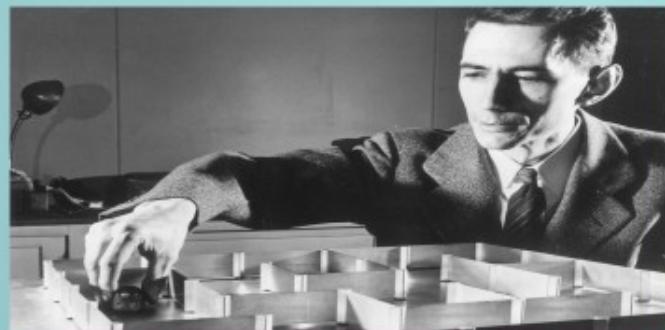
Armistizio 11 novembre 1918





## CLAUDE SHANNON

Nacque negli USA il 30 aprile 1916 a Petoskey, capoluogo del Michigan. Oltre ad essere un lontano parente di Thomas Edison fu un ottimo studente e già a 20 anni aveva ben due lauree conseguite nell'università del Michigan: matematica e ingegneria elettronica. Subito dopo la laurea si iscrisse al MIT.

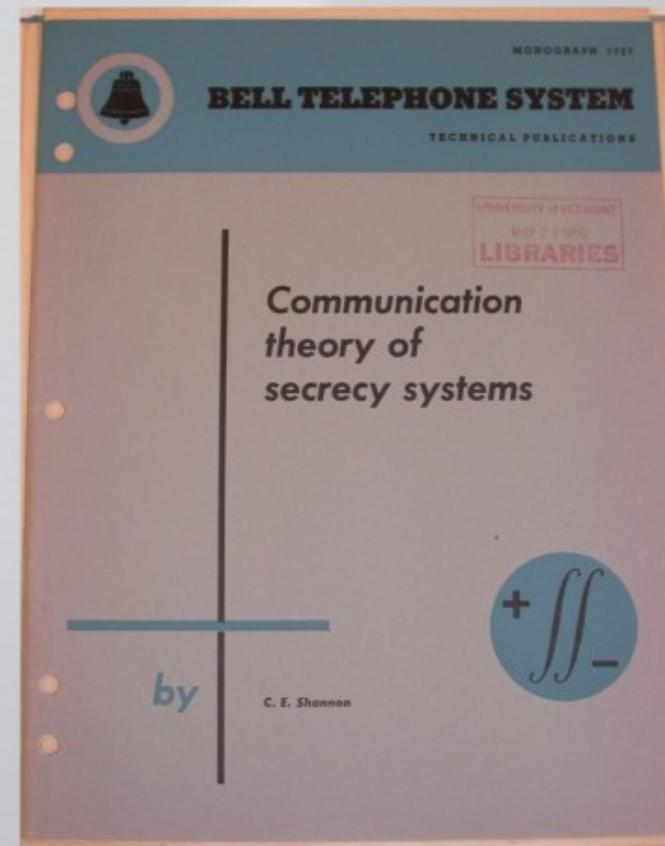


CRITTOGRAFIA

TEORIA  
DELL'INFORMA  
ZIONE

# CRITTOGRAFIA

Nel 1949 Claude Shannon pubblicò l'articolo “La teoria della comunicazione nei sistemi crittografici” con il quale praticamente fondò la teoria matematica della crittografia.



# Crittografia

La parola crittografia deriva dal greco “*kriptòs*” (nascosto) e “*gràphein*” (scrivere); l’insieme vuol dire scrittura nascosta, cioè non leggibile da chi non autorizzato.

Le reti per loro natura non sono sicure infatti, se le comunicazioni non sono crittografate, basta un semplice analizzatore di rete per intercettare le informazioni che viaggiano.



# I problemi da risolvere

- **Segretezza:** informazioni leggibili solo da chi autorizzato
- **Autenticazione:** evitare che malintenzionati si spaccino per qualcun altro
- **Affidabilità:** garantire che l'informazione non arrivi alterata al destinatario



# Cifratura

Testo in chiaro (plain text)

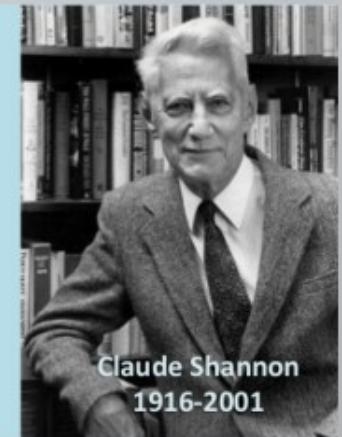
algoritmo di cifratura

Testo cifrato (cipher text)

Questo processo viene chiamato **cifratura** e deve essere noto da entrambi gli interlocutori (il mittente cifra, il destinatario decifra).

Il processo di cifratura è composto da due parametri: l'**algoritmo** e la **chiave**. La cifratura deve dipendere interamente dalla chiave (princípio di Kerckoffs)

"The enemy knows the system being used."  
Claude Shannon,  
*Communication Theory of Secrecy Systems*  
(1949)



Claude Shannon  
1916-2001

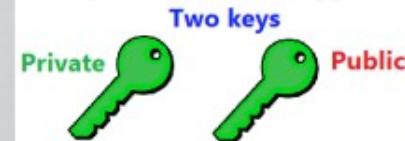
# Tipi di cifratura

- **Chiave simmetrica**: la chiave di cifratura corrisponde a quella di decifratura
- **Chiave asimmetrica** dove per cifrare e decifrare vengono utilizzate due chiavi diverse.

Symmetric Encryption



Asymmetric Encryption



Una ulteriore classificazione può essere fatta in base al tipo di dato su cui lavorano:

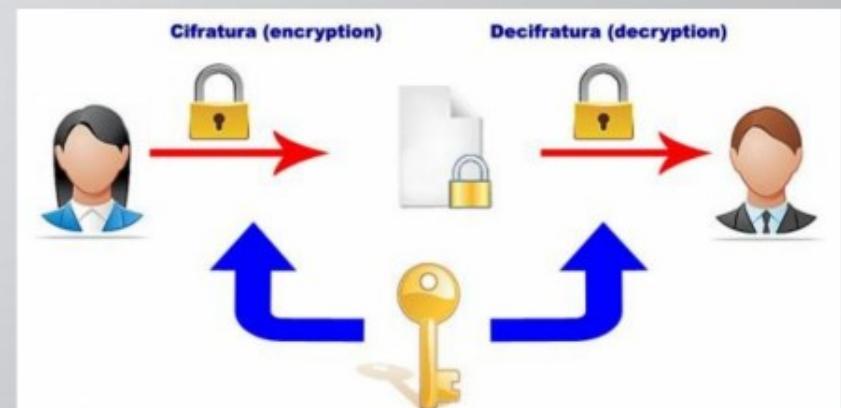
- **block cipher** dividono il messaggi in blocchi e ogni blocco viene crittografato
- **stream cipher** ogni singola unità di informazione (bit o byte) viene combinata con la chiave.

# Crittografia simmetrica

La crittografia simmetrica, o crittografia a chiave privata, è una tecnica di cifratura.

**Pro:** semplice, molto performante e facile da implementare.

**Contro:** presuppone che le due parti siano già in possesso delle chiavi, richiesta che non rende possibile uno scambio di chiavi con questo genere di algoritmi.

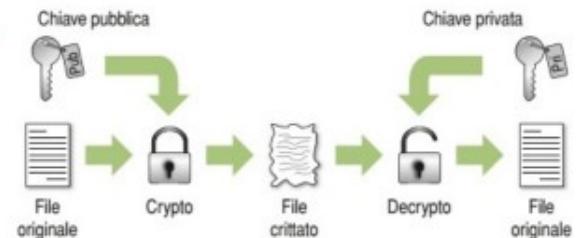


# Crittografia asimmetrica

Nata per risolvere il problema dello scambio della chiave, l'idea di base di questa tecnica crittografica è avere, per ogni utente, due chiavi diverse dette **chiave pubblica** e **chiave privata**, quest'ultima deve essere tenuta nascosta.

Abbiamo quindi due modalità di funzionamento:

- 1 **modalità confidenziale:** sono garantite la **riservatezza** e l'**integrità** del messaggio;



- 2 **modalità autenticazione:** garantisce l'**integrità** e il **non ripudio** ma non viene garantita la **riservatezza** (il mittente ha posto la sua **firma elettronica** sul messaggio).



# Crittografia ibrida

La crittografia asimmetrica però è molto lenta quindi la tecnica più usata oggigiorno è la **crittografia ibrida** con cui due utenti si scambiano una *chiave di sessione* tramite la *crittografia asimmetrica*; una volta in possesso della stessa chiave di sessione possono scambiarsi messaggi con la stessa chiave quindi usando la crittografia simmetrica.



# Firma digitale

Garantisce l'integrità e l'autenticazione.

1. Viene calcolato l'hash (fingerprint o digest) del messaggio
2. Viene crittografato il messaggio con la chiave pubblica del destinatario
3. Il digest viene crittografato con la propria chiave privata
4. Il digest viene accodato al messaggio e spedito.
5. Il destinatario decrittura il messaggio con la propria chiave privata
6. Il destinatario decrittura il digest con la chiave pubblica del mittente
7. Il destinatario adesso ha l'hash in chiaro e può procedere con la verifica



# Certificati digitali

Chi gestisce le chiavi pubbliche?

- Certification Authority (CA): rilasciano, pubblicano, validano (con la propria chiave privata) i certificati
- Registration Authority (RA): verificano l'identità del soggetto che richiedere il certificato

La PKI (Public Key Infrastructure) è il repository dei certificati.



# TEORIA DELL'INFORMAZIONE

*“Informazione è tutto ciò che aumenta la nostra conoscenza”*

*“Un dato rilevato dal mondo che ci circonda rimane tale fino a quando non riusciamo a dargli un significato, a quel punto diventa informazione”*



# TEORIA DELL'INFORMAZIONE

*“Informazione è tutto ciò che aumenta la nostra conoscenza”*

*“Un dato rilevato dal mondo che ci circonda rimane tale fino a quando non riusciamo a dargli un significato, a quel punto diventa informazione”*



**Ma come trasferiamo le informazioni?**

# Teoria dell'informazione

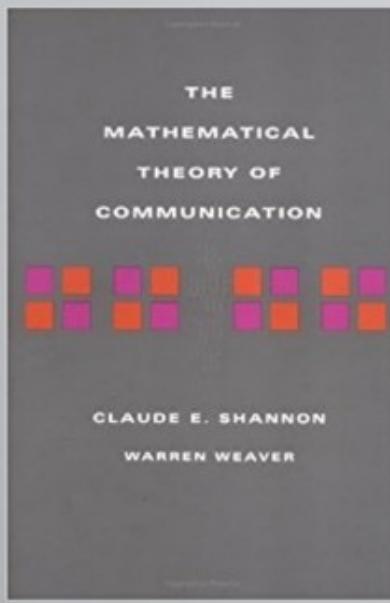
Prima di passare nel **canale**, l'informazione deve essere codificata in modo *efficace* ed *efficiente* dal **codificatore** in modo che alla destinazione il **decodificatore** sia in grado di ricostruire il messaggio e, nel caso di eventuali errori, correggerli.



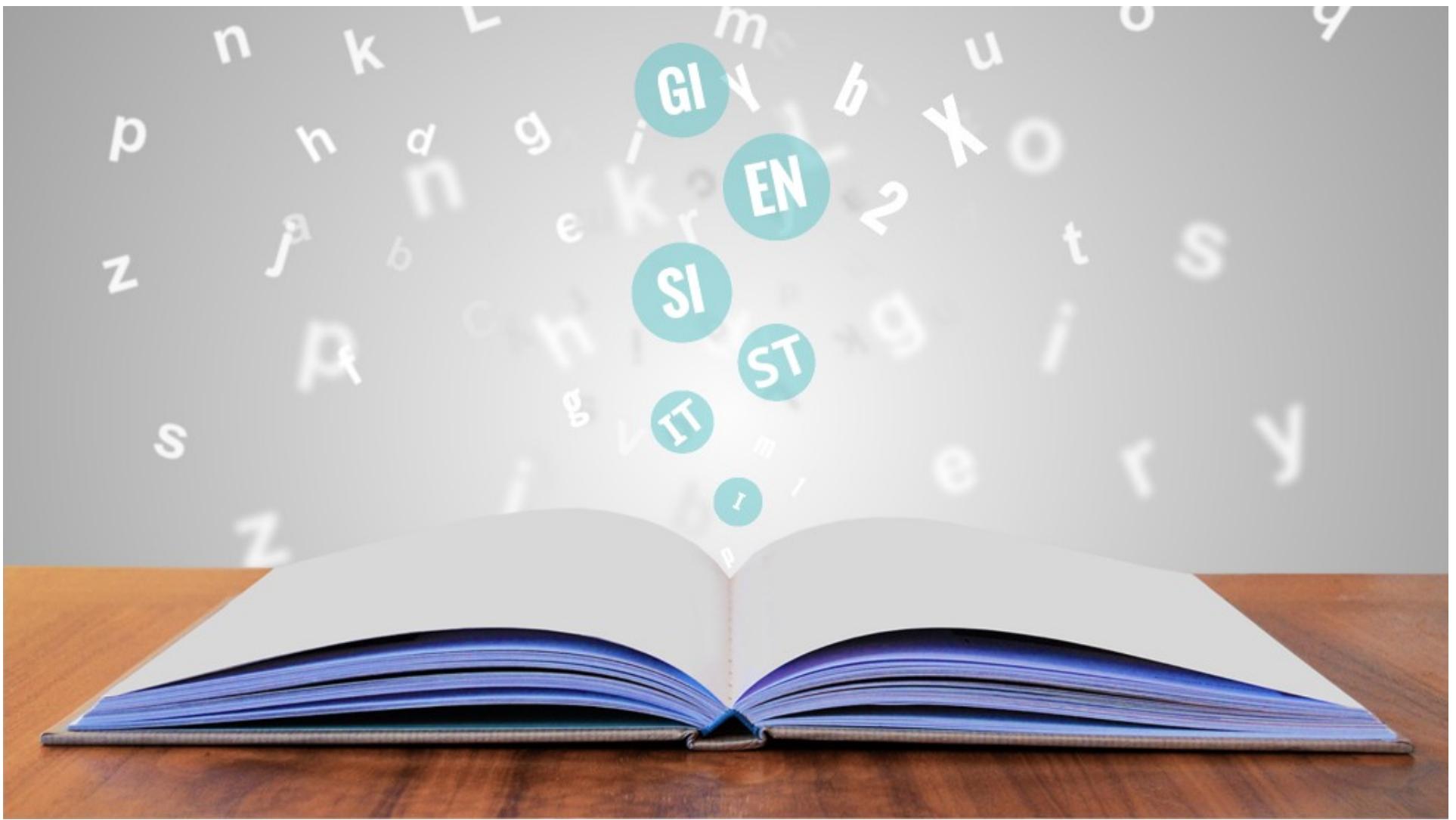
modello Shannon-Weaver

# Definizione

La teoria dell'informazione è una disciplina dell'informatica e delle telecomunicazioni che ha come scopo la quantificazione della quantità di dati (ossia di informazione) in relazione alla loro memorizzazione o trasmissione su un canale in modo affidabile.



Si considera come nascita della teoria dell'informazione la pubblicazione del lavoro "A Mathematical Theory of Communication" da parte di Claude Shannon



# **Wired and Wireless Media**

The data/information travel on a media that can be wired or wireless.



**Wired  
media**

**Wireless  
media**

# Wired media

In wired media the link between two or more devices is realized via physical wire

- Twisted pair → two wires twisted together to avoid interferences
- Coaxial cable → central copper core surrounded by an insulating layer and all enclosed by a shield
- Fiber-optic cable → composed of hundreds of glass or plastic fibre strands usually to transmit light



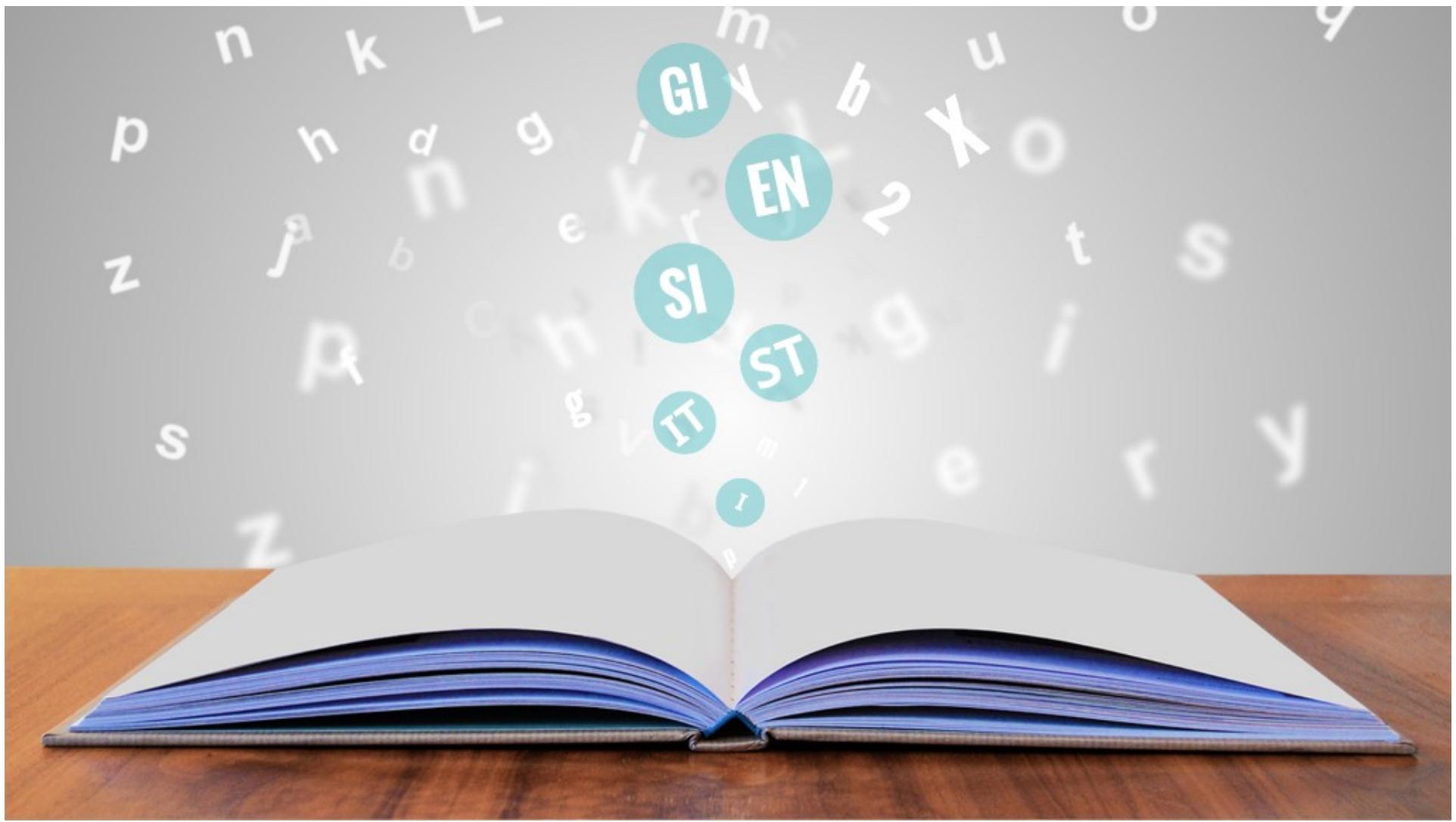
# Wireless media

Wireless media are media that do not need a wire in order to transmit data, instead they use electromagnetic waves that propagates in the space.

- Infrared → higher frequency than radio waves. They send data as light rays and can be used only in line of sight.  

- Radio frequency → Radio communication can carry information up to kilometres and can surpass obstacle. Interferences and bad weather can cause problems.  

- Microwave → higher frequency than radio waves but lower than infrared. Microwaves unlike radio waves have difficulty to surpass walls or obstacle so it is better use them only in line of sight  

## L'INFORMAZIONE E L'ORGANIZZAZIONE

In un'organizzazione l'informazione è tutto ciò che concerne un'azienda come progetti e piani attuali e futuri, i dati degli utenti o le analisi di mercato.



GLI STRUMENTI  
INFORMATICI

L'IMPRESA

# GLI STRUMENTI INFORMATICI

- Tecnologie informatiche di automazione:



- Tecnologie informatiche di supporto alle decisioni:



- Tecnologie informatiche embedded:



- Tecnologie informatiche infrastrutturali:



# L'IMPRESA

L'impresa è un organizzazione di persone e beni economici istituita per il conseguimento di un determinato scopo.



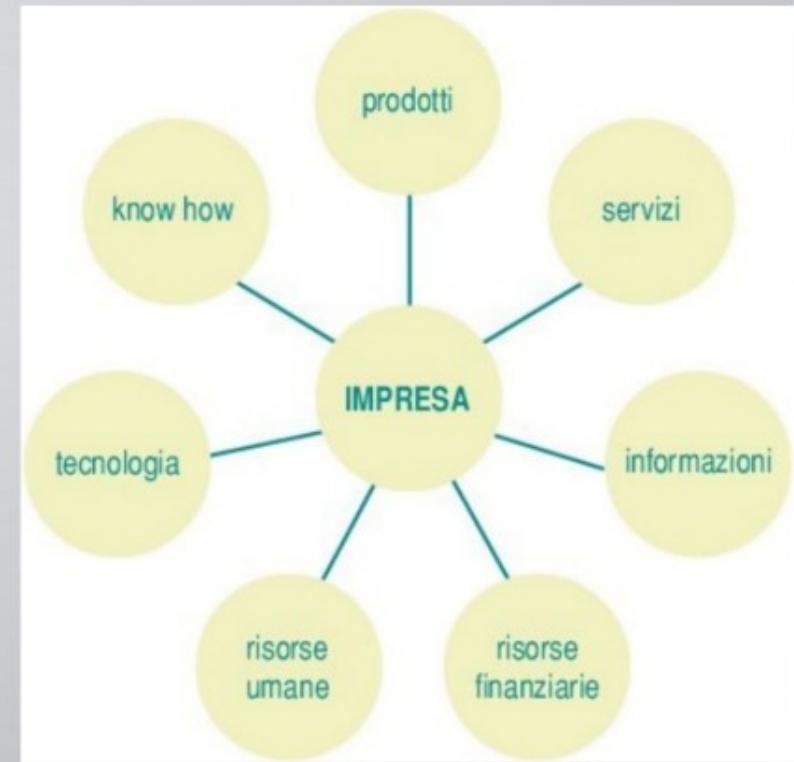
Il sistema  
azienda

Suddivisione  
del lavoro

Meccanismi di  
coordinamento

# Il sistema azienda

Intorno all'impresa ruotano 7 concetti chiave che la rendono un sistema più complesso, quindi bisogna sapere **organizzare** cioè decidere chi fa cosa.



# Suddivisione del lavoro

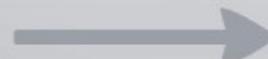
In un'azienda bisogna quindi suddividere il lavoro e una prima suddivisione può essere in base alla specializzazione:

- Specializzazione verticale: controllo che una certa posizione ha sulla esecuzione dei propri compiti.
- Specializzazione orizzontale: numero di compiti che sono assegnati ad una certa posizione.



alienazione, demotivazione

Per contrastare l'eccessiva specializzazione si attuano delle contro misure



# Meccanismi di coordinamento

- **Ex-post:** le esigenze organizzative vengono risolte sul momento.
- **Ex-ante:** le esigenze organizzative vengono pianificate a priori.



