*Percorso Multimediale dell'alunno*
***Maglieri Roberto***
***Classe 5° A scientifico***
***IISS "L. da Vinci" – Fasano (BR)***

# Infosec:
# la comunicazione attraverso Onde ed Enigmi

***STORIA:*** "Il Codice Enigma"

***FISICA:*** "La trasmissione delle informazioni attraverso onde ELM"

***GEOGRAFIA ASTRONOMICA:*** "La propagazione delle onde ELM"

***LATINO:*** "Il Quinto Elemento: l'Etere"

***ITALIANO/ATTUALITA':*** "Privacy e sicurezza dei dati"

***INGLESE:*** "Big Brother is watchin' you!" from "1984" by G. Orwell

***FILOSOFIA:*** "La comunicazione ed il linguaggio"

***ESAME DI STATO a.s. 2004/2005***

# INFOSEC: LA COMUNICAZIONE ATTRAVERSO ONDE ED ENIGMI

Argomento della tesina è la comunicazione attraverso l'impiego di onde elettromagnetiche opportunamente codificate. Il tutto si sviluppa in sette sezioni, ciascuna delle quali analizza l'argomento da un punto di vista "disciplinare" diverso:

- STORIA: Il Codice Enigma
- FISICA: La trasmissione delle informazioni attraverso onde ELM
- GEOG.AST. La propagazione delle onde ELM
- LATINO Il Quinto Elemento: l'Etere
- ITALIANO Privacy e sicurezza dei dati
- LETT.INGL "Big Brother is watchin' you!" from "1984" by G. Orwell
- FILOSOFIA La comunicazione ed il linguaggio

La sezione tecnica è accompagnata da opportune trattazioni in ambito di Filosofia (Comunicazione e linguaggio), Italiano/Attualità (Privacy e sicurezza dati) e riferimenti alla Letteratura Inglese ("1984" di G. Orwell).
La tesina è stata realizzata in formato multimediale utilizzando tecnologie quali Flash MX integrato con HTML, suoni e filmati.

## SEZIONE 1: IL CODICE ENIGMA

Nella prima sezione viene presentato il "codice Enigma" e le conseguenze storiche che derivarono dal suo utilizzo. Del "codice/macchina Enigma" vengono descritte **l' ideazione**, originariamente per uso civile; **il funzionamento**, la costruzione meccanica; i primi tentativi di **decifrazione** da parte dei Polacchi e dell'Intelligence britannica ed infine la costruzione dei **calcolatori/decifratori elettromeccanici** "Colossus", ideati da *Alan Turing*, tra i padri fondatori dell'informatica teorica. Viene, infine, fornita una **simulazione elettronica** dell'Enigma realizzata in Flash.

## SEZIONE 2: LA TRASMISSIONE DELLE INFORMAZIONI ATTRAVERSO ONDE ELM

Nella seconda sezione, dopo aver presentato alcune **nozioni utili** in ambito fisico (frequenza, lunghezza d'onda, spettro elettromagnetico). Viene svolta un'**analisi costi-benefici** sulle attuali modalità di trasmissione delle informazioni attraverso le onde elettromagnetiche:
- la propagazione nello spazio (irradiazione);
- la trasmissione su linea e guida d'onda;
- la trasmissione su fibra ottica.

## SEZIONE 3: LA PROPAGAZIONE DELLE ONDE ELM

La terza sezione tratta della propagazione delle onde elettromagnetiche, introducendo ed analizzando il particolare fenomeno della "riflessione della Ionosfera" e definendo le caratteristiche principali di questa parte di atmosfera (struttura "a strati", ionizzazione, connessioni con i cicli solari). Si fanno, inoltre, brevi **cenni alla Protezione Civile**, in cui l'utilizzo delle radiocomunicazioni è rilevante per un efficace coordinamento delle unità operative.

**SEZIONE 4: IL QUINTO ELEMENTO: L'ETERE**

Nella quarta sezione viene presentato il concetto di "etere", già affrontato nei tempi antichi da scienziati/filosofi del mondo greco (Aristotele nel "Meteorologica") e latino (Seneca nelle "Naturales Quaestiones" e Plinio il Vecchio nel "Naturalis Historia"). Queste opere ci forniscono una chiara testimonianza delle **conoscenze scientifiche** di quei tempi.

**SEZIONE 5: PRIVACY E SICUREZZA DEI DATI**

La sezione quinta affronta il problema della **tutela della privacy** nella Costituzione Italiana (art.15) e illustra le **violazioni quotidiane** perpetrate ai danni del cittadino, ad esempio con la videosorveglianza, le tecnologie digitali (TV interattiva, carte di identità e passaporti elettronici…), lo "sniffing" nella navigazione in internet (la "cattura" di passwords, email, dati delle carte di credito ecc.), e la "lettura" degli stili di vita di ciascuno di noi tramite la "tracciatura" dei percorsi dei prodotti commerciali (etichette intelligenti, acquisti on line, ecc…).

**SEZIONE 6: "BIG BROTHER IS WATCHING YOU"**

Nella sesta sezione vengono discusse le **violazioni alla "privacy** ampiamente analizzate da *George Orwell* nell'opera "*1984*", romanzo anti-utopico in cui l'autore descrive una macabra civiltà occidentale soggiogata da una dittatura totalitaristica, ove la condizione dell'uomo ridotto all'estremo dell'abiezione e della capitolazione della propria dignità è rappresentata sotto una luce sinistra dominata dall' onnipresente immagine del "Grande Fratello".

**SEZIONE 7: LA COMUNICAZIONE ED IL LINGUAGGIO**

Nell'ultima sezione, viene affrontato il tema della definizione filosofica del **linguaggio** e della **comunicazione**, secondo l'interpretazione del *Circolo di Vienna*, da cui scaturì una corrente di pensiero nota come **Neopositivismo.** Scopo di questa corrente era quello di costruire un nuovo linguaggio scientifico assolutamente corretto ed "oggettivo", estensibile a tutte le scienze.
Viene, inoltre, presentato il tentativo di "connessione" col pragmatismo americano effettuato da *Charles Morris*, studioso del linguaggio, il quale afferma che l'indagine semiotica non deve ridursi esclusivamente all'analisi del linguaggio scientifico, bensì estendersi a tutti i diversi usi linguistici. Morris attribuisce alla **semiotica** la funzione di "**tutela della libertà dell'individuo**" in una società in cui si è sempre più condizionati, fino a subire un autentico assedio da parte della pubblicità e della propaganda.

# INFOSEC:
# LA COMUNICAZIONE ATTRAVERSO ONDE EO &NIGMI

Chiudi

- Il codice Enigma
- La trasmissione delle informazioni
- Propagazione delle onde ELM
- Il Quinto Elemento
- Privacy e sicurezza dei dati
- Il linguaggio e la comunicazione
- *Quotes & Credits*


*Tesina Multimediale*

*Magliari Roberto*

*classe 5° A sc.  a.s. 2004/2005*

A

Chiudi

# COSA E' ENIGMA?

L'Enigma fu una macchina per cifrare (e decifrare) elettro-meccanica, al servizio delle Forze Armate tedesche. La sua facilità d'uso e la supposta indecifrabilità furono le maggiori ragioni per il suo ampio utilizzo.

Il progetto originale, sviluppato da Arthur Scherbius, era per una macchina "civile" che serviva per evitare lo spionaggio industriale.

Già nel 1° Conflitto Mondiale, i vertici delle Forze Armate tedesche utilizzavano Enigma per cifrare le missive.
Acquisito nel 1929 dalla Marina Militare Tedesca,
venne poco a poco implementata in tutte la gerarchia nazista.

Next

A

Chiudi

# FUNZIONAMENTO DI ENIGMA

La macchina Enigma aveva l'aspetto di una macchina da scrivere con due tastiere: una, vera, e la seconda fatta di lettere luminose.
Il suo funzionamento si basava su tre dischi cablati,detti rotori, che avevano 26 contatti per lato (uno per ogni lettera dell'alfabeto tedesco): il primo disco ruotava di una lettera ad ogni pressione di tasto, il secondo ruotava di una lettera ogni volta che il primo compiva un giro e il terzo ruotava di una lettera quando il secondo finiva un giro. Il terzo e ultimo rotore era collegato a un riflettore.
Oltre a questo, Enigma poteva essere regolata con degli spinotti per scambiare fra loro dieci lettere con altre dieci a scelta.

I risultati apparivano illuminati sulla tastiera apposita, lettera dopo lettera, e una persona doveva provvedere a trascriverli a mano su un foglio di carta.


La chiave dell'Enigma è la disposizione iniziale dei rotori;
questa chiave veniva cambiata ogni 24 ore secondo una regola prefissata.

Back

Next

A

Chiudi

# DECIFRARE ENIGMA

I primi a decifrare i messaggi in codice di Enigma furono un gruppo di matematici polacchi. Nel 1938 l'intelligence polacco progettò una macchina apposita, chiamata Bomba.

Il progetto venne passato agli inglesi nel 1939, che organizzarono una attività di intercettazione e decifrazione delle comunicazioni radio tedesche a Bletchley Park.

In realtà il primo a violare l'impenetrabile segretezza di Enigma fu la spia Hans Thilo Schmidt, funzionario del ministero della Difesa tedesco, che già nel 1931 aveva venduto ai servizi segreti francesi alcuni manuali del sistema cifrato.

I tedeschi non arrivarono mai a dubitare dell'invulnerabilità del loro codice e per tutta la durata della guerra continuarono a comunicare sulla base di Enigma.

A

Chiudi

# DECIFRANDO ENIGMA

Il codice Enigma fu decodificato attraverso il primo calcolatore elettromeccanico della storia:

"Colossus"

(entrato in funzione nell'anno 1943)

L'ideatore di questo calcolatore è Alan Turing, brillante matematico, tra i padri fondatori dell'informatica teorica per le sue straordinarie teorie sull'A.I. (Turing Test), e sul computer (Turing Machine).
Venne "arruolato" dall'Intelligence britannica allo scoppio della guerra assieme a molti altri fisici, matematici, scacchisti.
Il compito di questa équipe era quello di costruire un qualcosa in grado di decodificare in tempo reale un messaggio codificato con Enigma.

L'apparecchio che l'Intelligence aveva sino ad allora usato, si chiamava "Ultra" e la sua importanza fu determinante nel mediterraneo e nel Nord Africa.

Back

Next

# Trasmissione tramite Onde ELM

## Nozioni utili...

Frequenza:
- E' il numero di cicli effettuati da un sistema/quantità periodica nell'unità di tempo;
- Si misura in Hertz (Hz);

$f = 1 / t$ $\qquad$ $f = \omega / 2\pi$

Lunghezza d'onda:
- E' la distanza fra due punti aventi la stessa fase in 2 cicli consecutivi di un'onda periodica, nel verso di propagazione;
- Si misura in m, cm, nm... [L]
- Si indica con $\lambda$ (LAMBDA)

**RELAZIONE FONDAMENTALE:** $\lambda = c / f$


Spettro Elettromagnetico: Insieme delle onde elettromagnetiche di tutte le lunghezze d'onda. Lo spettro elettromagnetico comprende le onde radio, gli infrarossi, la luce visibile, gli ultravioletti, i raggi X e i raggi gamma.

# Trasmissione tramite Onde ELM

- PROPAGAZIONE NELLO SPAZIO (IRRADIAZIONE)
- TRASMISSIONE SU LINEA E GUIDA D'ONDA
- TRASMISSIONE SU FIBRA OTTICA

# Trasmissione tramite Onde ELM

## PROPAGAZIONE NELLO SPAZIO (IRRADIAZIONE)

CANALE: Etere
TRASMISSIONE: Antenna
RICEZIONE: Antenna


### 3 TIPI DI PROPAGAZIONE:

- Propagaz. via onde terrestri ( < 300 KHz )
- Propagaz. via riflessione IONOSFERA ( 300 KHz < x < 3 GHz )
- Propagaz. diretta ( < 3 GHz fino a 300 GHz )

### APPLICAZIONI

Radiofonia, Radiocomunicazioni, TV, Cellulari, Satelliti, Radar

| PRO | & | CONTRO |
|---|---|---|
| - Lunghe distanze | | - Inquinamento elettromagnetico |
| - Bassi costi | | - Interferenze |
| - Apparecchiature poco complesse | | - Poca sicurezza / privacy |
| | | - Grandi dimensioni |

Back Next

# Trasmissione tramite Onde ELM

## TRASMISSIONE SU LINEA E GUIDA D'ONDA

CANALE: Mezzo metallico (filo, cavo coax)
TRASMISSIONE: Trasmettitore
RICEZIONE: Ricevitore

- Trasmissione del segnale (l'informazione) attraverso onde di corrente o tensione.

- Frequenze da 1 GHz a 900 GHz

### I CANALI

Doppino telefonico, cavo coassiale, circuiti elettronici, microstriscia, guide d'onda

| PRO | & | CONTRO |
| --- | --- | --- |
| - Massima privacy | | - Basse distanze |
| - Buona velocità | | - Attenuazione e distorsione |
| - NO interferenze | | - Sistema complesso |
| - Piccole dimensioni | | |

# Trasmissione tramite Onde ELM

## TRASMISSIONE SU FIBRA OTTICA

CANALE: Dielettrico (fibra ottica)
TRASMISSIONE: Led, Laser
RICEZIONE: Photodetector

- Trasmissione del segnale (l'informazione) con impulsi di luce intorno alle frequenze 1 THz - 100 THz.
- Lavoro nell'ordine di grandezza dei micrometri ( $10^{-6}$ ) e nanometri ($10^{-9}$ )
- Evoluzione recente ( 1970 --> Sperimentazione  2000 --> Diffusione commerciale )

**PRO**

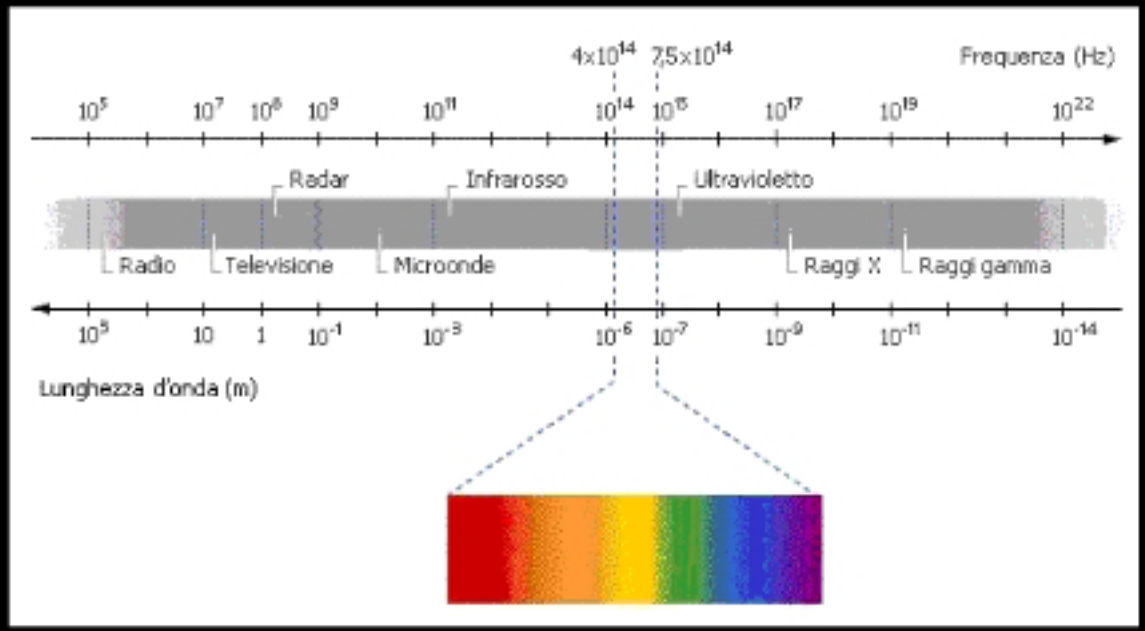
- Altissima velocità e capienza (Banda UTILE)
- Altissima affidabilità
- Dimensioni SUPER-ridotte

**&**

**CONTRO**

- Tecnologia molto COMPLESSA e DELICATA
- Elevato costo
- Non DIRETTAMENTE interfacciabile ai sistemi elettrici (Regime OTTICO <--> Regime ELETTRICO)

# Trasmissione tramite Onde ELM



# Trasmissione tramite Onde ELM

# Trasmissione tramite Onde ELM

| Frequenza | Definizione | Utilizzo tipico |
|---|---|---|
| 3 – 30 kHz | Very Low Frequency (VLF) | Navigazione, sonar |
| 30 – 300 kHz | Low Frequency (LF) | Segnali radio, soccorso navale |
| 300 – 3000 kHz | Medium Frequency (MF) | Trasmissioni radio AM, comunicazioni navali, comunicazioni della Guardia costiera, orientamento |
| 3 – 30 MHz | High Frequency (HF) | Comunicazioni internazionali ad onde corte; radio amatori; comunicazioni nave-costa, nave-velivoli |
| 30 – 300 MHz | Very High Frequency (VHF) | Televisione, trasmissioni radio FM, controllo del traffico aereo, polizia, soccorso navale |
| 300 – 3000 MHz | Ultrahigh Frequency (UHF) | Televisione, comunicazioni satellitari, radiosonde, radar di sorveglianza, soccorso navale; comunicazioni mobili (GSM, etc.) |
| 3 – 30 GHz | Superhigh Frequency (SHF) | Radar per aviotrasporti, collegamenti a microonde, comunicazioni satellitari |
| 30 – 300 GHZ | Extremely High Frequency (EHF) | Radar, esperimenti |

In questo preciso istante, nell'etere intorno a noi, migliai di informazioni, dati, suoni vengono trasmesse via radio da un punto all'altro della Terra.

## CENNI DI FISICA

Quando una corrente elettrica variabile percorre un conduttore elettrico, crea nello spazio circostante una perturbazione magnetica.
I valori della corrente elettrica e del campo magnetico sono proporzionali tra loro.

Se ad un generatore di corrente colleghiamo un'antenna, il campo elettrico si propaga nello spazio circostante sotto forma di energia elettromagnetica, definita ONDA, che si allontana a velocità vicina a quella della luce.
Se ad una certa distanza dall'antenna trasmittente, si pone un conduttore metallico (ricevente), questo sarà "investito" dall'energia elettromagnetica;
tale energia genererà una corrente elettrica con caratteristiche simili a quella trasmessa.

Queste Onde Radio, si propagano attraverso l'aria, il vuoto, i liquidi,al di fuori dell'atmosfera terrestre, sempre in linea retta.
Grazie ad un particolare fenomeno (Riflessione della ionosfera), si riesce a superare ostacoli e la curvatura terrestre.

## LA IONOSFERA

Parte di atmosfera posta compresa tra i 50-70 km (MESOSFERA) e gli strati più alti della TERMOSFERA (400-500 km) caratterizzata dalla presenza di cariche elettriche (ioni) prodotte da radiazioni X ed ultraviolette solari e raggi cosmici.
Questa struttura "a strati" ionizzata, influenza la propagazione delle onde radio che vengono riflesse, consentendo le radiocomunicazioni a grande distanza.
La "riflessione" è strettamente legata ai cicli solari.
Nella Ionosfera si formano, inoltre, le aurore polari, anche queste ultime connesse alle perturbazioni emanate dal Sole.

# QUANDO E PERCHE' COMUNICARE ATTRAVERSO ONDE ELM

## CENNI DI PROTEZIONE CIVILE

In casi di emergenza "non gravi":

--> Saturazione rete GSM (cellulari)

--> Mancanza copertura GSM (zone d'ombra...)

In casi di emergenza "gravi":

--> Collasso rete GSM

--> Saturazione o collasso linee telefoniche "fisse"

++ Collegamenti tra strutture di comando e quelle operanti sul luogo dell'incidente;

++ Collegamenti tra le singole unità operative;

++ Utile alla propria sicurezza, in caso di necessità.

I

Aristotele affermava che:
"..il mondo sublunare è costituito da un quinto elemento, privo di peso e dotato di movimento circolare : di esso sono dotati i corpi celesti." *(Meteorologica)*

Anche Seneca, nelle Questioni Naturali (Naturales Quaestiones), opera "tarda" di argomento scientifico, tratta di fenomeni atmosferici e celesti, proponendo, inoltre, disgressioni di carattere moralistico.

Mirando all'utilità pratica del lettore ed anteponendo la *utilitas iuvandi* alla *gratia placendi*, Plinio il Vecchio raccoglie nella Naturalis Historia (Scienze Naturali) più di duecento manoscritti, destinati ai tecnici e agli studiosi.
La selezione dei dati é così rigorosa, che fu definita "inventario del mondo".

Pur essendo entrambi convinti assertori della ricerca scientifica, assumono un atteggiamento anti-tecnologico.

# Privacy e sicurezza dei dati

## COSTITUZIONE DELLA REPUBBLICA ITALIANA

Art. 15.

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

# Privacy e sicurezza dei dati

## "1984" di George Orwell diventa Realtà!

## BIG BROTHER IS WATCHIN' YOU!

| | |
|---|---|
| Per strada: | 1000 telecamere sulla città... (videosorveglianza) |
| A casa: | La TV "interattiva" |
| Comunicazioni: | Tracing cellulari<br>Registrazione telefonate |
| Acquisti: | Dati commerciali / Carte di credito<br>Etichette "intelligenti" |
| Dati personali: | Passaporto / Tess. Sanitaria / Carta Identità elettronici |
| Sulla Rete: | Tracing e-mail / Acquisti on-line / Users & passwords |
| Le PP.AA.: | Fisco<br>Forze Armate |

Costituito nel 1924 ad opera di Moritz Schlick, il Circolo di Vienna divenne uno stabile gruppo di discussione che si riuniva per discutere sia di questioni generali di filosofia della scienza, sia del pensiero di Ernst Mach.
Il Circolo raccoglieva studiosi di varie discipline, che avevano in comune l'insoddisfazione per i risultati raggiunti fino ad allora dalla filosofia, l'ammirazione per il metodo scientifico, il rifiuto per le diverse forme di metafisica, l'interesse per la matematica, la logica e la fisica teorica.
Da questo gruppo si sviluppò una corrente di pensiero che divenne nota come Neopositivismo.
Nel 1929, Hahn, Neurath e Carnap pubblicarono il manifesto del Circolo: "Una visione scientifica del mondo. Il Circolo di Vienna".
Per i neopositivisti di Vienna la fondazione del metodo scientifico era strettamente connessa con la costruzione di un linguaggio scientifico assolutamente corretto, una *lingua esatta delle scienze*.

La progressiva affermazione del nazismo in Germania e in Austria segnò la dispersione del Circolo di Vienna. Molti degli esponenti del gruppo emigrarono negli Stati Uniti, cercando di pubblicare una Enciclopedia delle scienze unificate a cui collaborarono anche N. Bohr, B. Russell e J. Dewey.
Essi entrarono in contatto con la filosofia pragmatistica, rappresentata oltre che da Dewey, anche da uno studioso del linguaggio, Charles Morris.
Morris tentò di creare una "connessione viennese" con il pragmatismo americano.
Egli affermava che le espressioni linguistiche devono essere ricondotte ai coimportamenti umani e che l'indagine semiotica non doveva ridursi all'analisi del linguaggio scientifico, ma estendersi a tutti i diversi usi linguistici.
Morris distingue, all'interno della semiosi, tre livelli di analisi:
1) Pragmatico-biologica (rapporto tra segni ed interprete);
2) Semantica (rapporto del segno al designatum);
3) Sintattica (relazioni dei segni tra loro).

Morris attribuisce alla semiotica la funzione di tutela della libertà dell'individuo, in una società in cui si è sempre più condizionati, fino a subire un autentico "assedio" da parte delle pubblicità e della propaganda.

*"Gli altri individui della società cercano di raggiungere i loro scopi invenstendoci con una continua pressione di segni, volti ad indicarci come agire, a cosa credere [..]*

*Ciascuno di noi tende a diventare un burattino mosso da segni, passivo nei riguardi delle nostre credenze, valutazioni ed attività."*

(tratto da "**Segni, Linguaggio, Comportamento**", C. Morris)

Bibliografia essenziale:

- Il Globo Terrestre e la sua evoluzione (5° ed.), Palmieri - Parotto, edit. Zanichelli
- Letteratura Latina 3 (nuova ed.), Giovanna Garbino, edit. Paravia

Siti web consultati:

- Wikipedia : l'Enciclopedia libera
- www.bletchleypark.org.uk
- www.bletchleypark.net
- Pianeta Radio
- Filosofico.net
- Kataweb - CittadinoLex

Realizzato da:

Roberto Maglieri (web-site / e-mail)

con Macromedia Flash MX PRO 2004