ISTITUTO MAGISTRALE STATALE
"REGINA MARGHERITA"
Licei: scienze umane, linguistico, economico sociale, musicale e coreutico
Piazzetta SS.Salvatore,1 – 90134 PALERMO
Tel. 091/334424 – Fax 0916512106
Codice fiscale 80019900820 – PAPM04000V
E – mail : papm04000v@istruzione.it

TITOLO: Codici e crittografia

Struttura:
Il modulo è strutturato in due fasi che affronteranno il pensiero computazionale e coding, finalizzate ad affrontare il tema della storia e analisi della crittografia, quanto mai attuale anche in relazione a importanti tematiche di cittadinanza digitale.
Nella prima fase si introdurranno i concetti fondamentali connessi al pensiero computazionale, dall'analisi di problemi per individuare le diverse tipologie (risolvibili, irrisolvibili, mal formulati), alla schematizzazione di un problema, la scomposizioni in un'unità problematiche, pianificazione progettuale di strategie risolutive, alla verifica della congruità e correttezza delle procedure.
L'esame e il metodo processuale di un problema specifico costruirà la competenza per la generalizzazione del metodo.
Nella fase successiva, anche attraverso strategie di gamefication, si elaboreranno e implementeranno procedure, in una scala di crescente complessità, per modellizzare codici crittografici di particolare rilievo dal punto di vista storico. Si accennerà a tal proposito ai precursori della macchina "Enigma", alla macchina "Enigma" e al ruolo di Touring nella storia dell'informatica e dall'automazione. Sarà interessante sottolineare
che alla crescente complessità procedurale corrisponde l'evoluzione storica delle strategie di criptazione e decriptazione.

Contenuti:
La progettazione si articolerà nei seguenti Passaggi:
Cenni sui principali operatori logici e schematizzazione circuitale;
Analisi delle differenti tipologie di azioni (in sequenza, in cicli definiti, indefiniti, scelte, eventi, attività in contemporanea).
Costruzione di un diagramma di flusso per il dettaglio del problema e l'impostazione dell'algoritmo: dalla modellizzazione all'implementazione;
Dall'implementazione al testing.
Specificatamente si affronteranno:
Il codice di Cesare, il disco cifrante di Leon Battista Alberti, il codice di Vigenère, metodi statistici per decriptare un testo, crittografica simmetrica, asimmetrica (RSA) e quantistica,
Il passaggio dalle chiavi private a quelle pubbliche e la segretezza delle informazioni.

Obiettivi generali:
Orientarsi in modo critico nel cyberspazio, con la consapevolezza degli strumenti e codici che ne costituiscono l'impalcatura;

Trasferire le competenze trasversali del pensiero computazionale in diversi ambiti del sapere e fattispecie esperienziale;
Sviluppare consapevolezza della pervasività dei messaggi crittografati nella vita di tutti i giorni e apprendere strumenti di interpretazione procedurale;
Sviluppare la capacità di interfacciarsi consapevolmente con strumenti digitali plugged e unplugged.

Obiettivi didattici formativi:
Saper traslare problemi in procedure e algoritmi, favorendo la costruzione di processi di transfert tra diversi campi disciplinari e/o diversi ambiti,
Saper usare un linguaggio di programmazione per la traduzione di un algoritmo e la sua implementazione;
Individuare un modello di codifica e implementazione di algoritmi per criptare e decriptare un testo;
Acquisire i principi base e gli obiettivi della crittografia: segretezza, integrità e autenticità delle informazioni;

Metodologia:
Il modulo sarà affrontato in un assetto laboratoriale proponendo procedimenti operativi di problem posing and solving e decision making, creando così i presupposti per stimolare abilità imprenditoriale nel quadro EQF.