

CriptoLab: alla scoperta della crittografia.

*Dalla teoria degli algoritmi al
coding crittografico*

Un'esperienza didattica innovativa per l'apprendimento
attivo degli **algoritmi crittografici**.

A cura di **Francesco Paolo Caforio**

Docente A-41 presso **I.I.S.S. "E. Majorana"** Martina Franca (TA)

Il contesto formativo

L'informatica oggi rappresenta una disciplina fondamentale che va ben oltre il semplice utilizzo di strumenti tecnologici. È una **scienza complessa** con linguaggi propri, modelli formali e profonde connessioni con la logica matematica.

Il laboratorio **CriptoLab** nasce in questa prospettiva innovativa, sostenuto dal **PNRR – DM 65/2023**, che promuove attivamente lo sviluppo delle competenze digitali e STEM attraverso metodologie didattiche all'avanguardia.



Perché la crittografia come strumento didattico?

$f(x)$

Matematica applicata

La crittografia offre un contesto concreto per applicare concetti matematici avanzati, dall'aritmetica modulare alla teoria dei numeri.



Informatica pratica

Gli algoritmi crittografici permettono di sperimentare direttamente con la programmazione, traducendo teoria in codice.



Rilevanza sociale

La protezione dei dati e la sicurezza delle comunicazioni sono temi che gli studenti vivono quotidianamente nella società digitale.

Obiettivi formativi del percorso

Teoria e pratica

Creare un ponte solido tra i *fondamenti teorici degli algoritmi* e la loro *implementazione* pratica attraverso la programmazione Python.

Competenze logico-matematiche

Potenziare il *ragionamento logico* e le capacità di *problem solving* attraverso l'analisi di problemi crittografici complessi.

Protezione dei dati

Comprendere i meccanismi fondamentali che garantiscono la *sicurezza delle informazioni* nel mondo digitale contemporaneo.

Autonomia progettuale

Sviluppare capacità di *progettazione autonoma* e *riflessione critica* sulle implicazioni tecnologiche e sociali.

Struttura organizzativa del laboratorio

30

Ore

Distribuite in 10 incontri
pomeridiani di 3 ore
ciascuno

30

Studenti

Del triennio dell'Istituto
Tecnico Informatica e del
Liceo Scienze Applicate

10

Incontri

Programmati con
progressione di
complessità crescente

Il percorso è stato progettato con una **progressione modulare**, partendo dai cifrari storici e arrivando gradualmente agli algoritmi moderni. Tutti i materiali didattici e i codici sviluppati sono stati organizzati in un **repository online** per garantire la **replicabilità** dell'esperienza.



Articolazione modulare del percorso

Modulo	Contenuti trattati	Attività e metodologie	Durata
<i>Crittografia</i>	Fondamenti, simmetrica e asimmetrica, applicazioni reali	Lezione dialogata, cooperative learning	3h
<i>Aritmetica modulare</i>	Conversioni, operazioni mod n, basi matematiche	Esercitazioni guidate, attività di gruppo	6h
<i>Cifrari classici</i>	Cesare, Vigenère, Vernam, crittoanalisi	Analisi di casi, codifica manuale, infografiche collaborative	6h
<i>Crittografia moderna</i>	DES, AES, RSA	Simulazioni, coding in Python, cooperative learning	6h
<i>Firma digitale</i>	Funzioni hash, autenticazione, blockchain	Esercitazioni pratiche, discussioni guidate	6h
<i>Monitoraggio</i>	Valutazione e riflessione finale	Autovalutazione, restituzione prodotti, metacognizione	3h





Fondamenti di crittografia

Il percorso didattico ha preso avvio dall'introduzione dei **concetti fondamentali della crittografia**, distinguendo chiaramente tra cifratura simmetrica e asimmetrica attraverso esempi pratici e contestualizzati.

1

Crittografia simmetrica

Stessa chiave per cifrare e decifrare.

2

Crittografia asimmetrica

Coppia di chiavi pubblico-privata.

3

Applicazioni reali

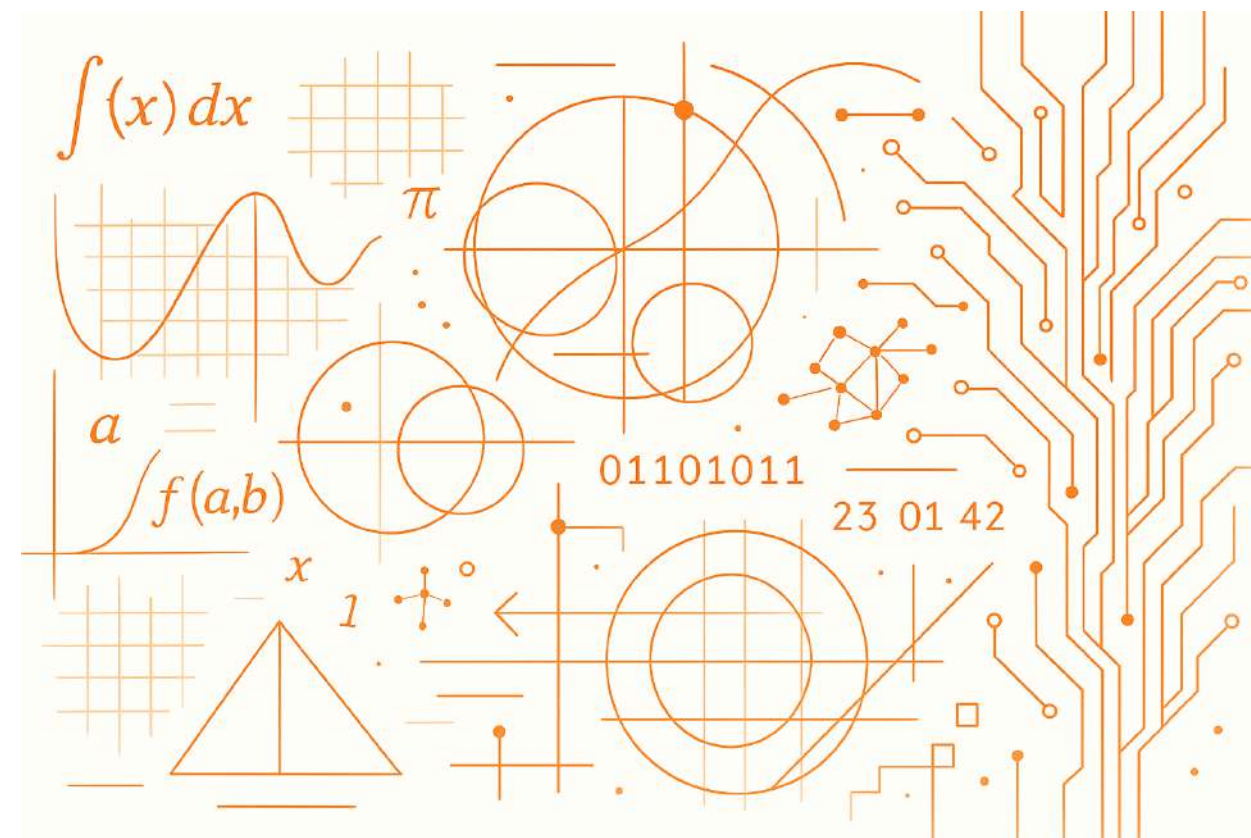
HTTPS, email sicure, pagamenti online, messaggistica crittografata nella vita quotidiana.

Aritmetica modulare: le basi matematiche

La componente matematica è stata affrontata attraverso un metodo **pratico e collaborativo**, focalizzandosi su:

- conversioni tra sistemi numerici
- operazioni aritmetiche modulo n
- proprietà fondamentali per la cifratura

Gli studenti hanno lavorato in **gruppi cooperativi** su problemi logici e matematici, sviluppando capacità di ragionamento sistematico e comprendendo come la matematica costituisca il fondamento teorico degli algoritmi crittografici.



❏ **Esempio pratico:** il cifrario di Cesare si basa su operazioni in aritmetica modulare, in cui lo spostamento delle lettere viene calcolato mod n .



Cifrari classici: dall'antichità alla modernità

Cifrario di Cesare

Spostamento fisso dell'alfabeto. Semplice da implementare ma vulnerabile all'analisi delle frequenze. Perfetto per comprendere i principi base della sostituzione.

1

Cifrario di Vernam

Basato sull'operazione XOR con chiave casuale. Teoricamente inviolabile se la chiave è lunga quanto il messaggio e usata una sola volta.

3

2

Cifrario di Vigenère

Cifrario polialfabetico con chiave ripetuta. Maggiore sicurezza rispetto a Cesare, ma ancora vulnerabile con tecniche avanzate di crittoanalisi.

Gli studenti hanno svolto **attività di crittoanalisi manuale**, imparando a identificare pattern, analizzare frequenze e valutare sistematicamente punti di forza e vulnerabilità di ciascun metodo crittografico.

Crittografia moderna: algoritmi del XXI secolo



Data Encryption Standard

Algoritmo simmetrico a blocchi da 64 bit con chiave da 56 bit. Analizzato in forma semplificata attraverso la struttura di Feistel e le operazioni di permutazione.



Advanced Encryption Standard

Successore del DES con blocchi da 128 bit e chiavi variabili. Esplorato attraverso simulazioni delle operazioni di sostituzione e trasposizione.



Rivest-Shamir-Adleman

Algoritmo asimmetrico basato sulla difficoltà di fattorizzare numeri primi grandi. Implementato in Python con esempi di generazione chiavi e cifratura.

L'approccio didattico ha privilegiato la **comprensione dei principi fondamentali** piuttosto che i dettagli implementativi, utilizzando simulazioni interattive, discussioni guidate e sessioni di coding collaborativo in Python.

Focus approfondito: algoritmo DES

L'**algoritmo DES** scomposto nelle sue componenti fondamentali per rendere comprensibile la logica interna di un algoritmo a blocchi moderno.

Permutazione iniziale

Riorganizzazione dei 64 bit di input secondo una tabella predefinita che separa i bit pari dai dispari.

16 round di Feistel

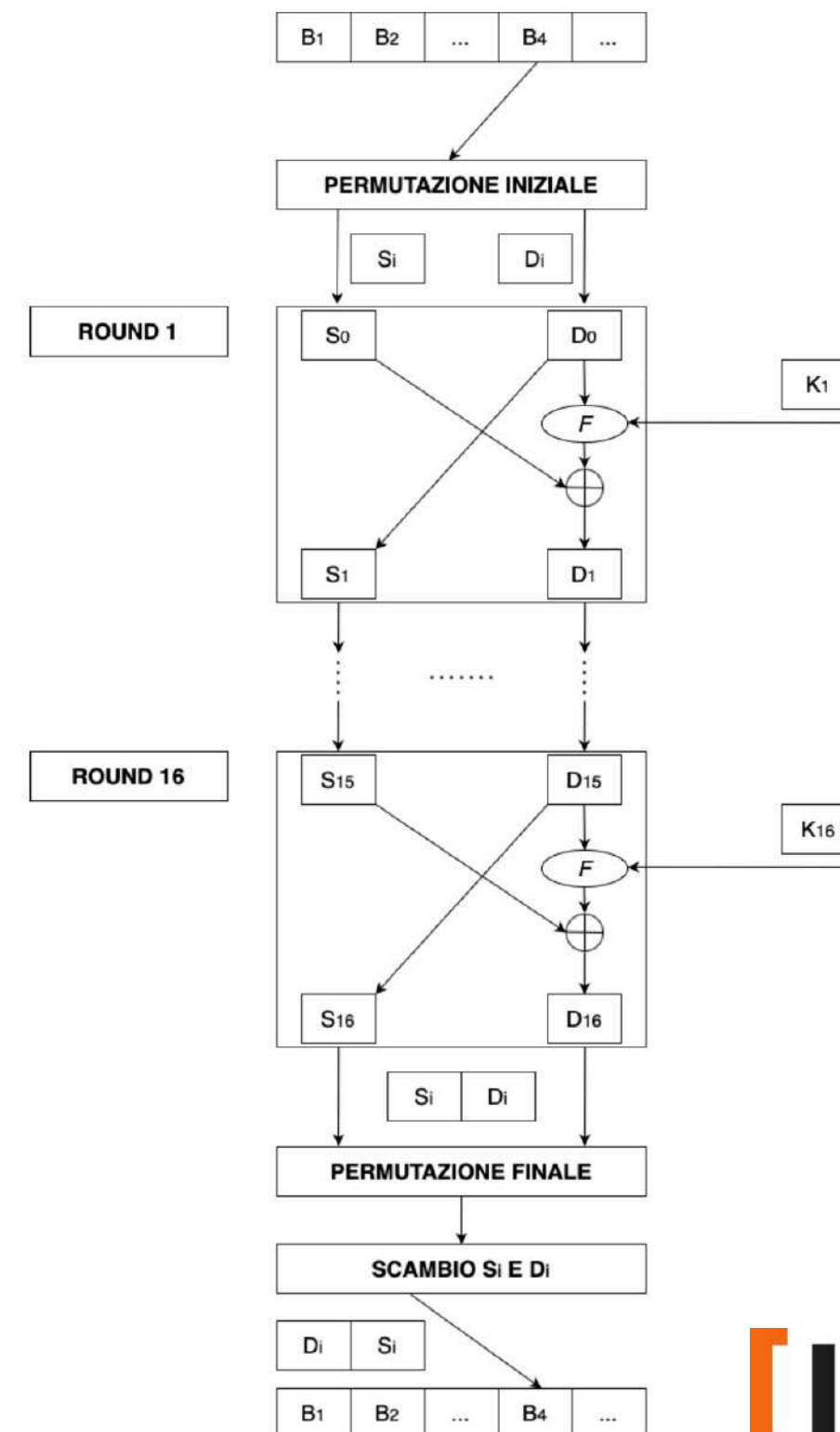
Operazioni cicliche che includono espansione, XOR con sottochiavi, sostituzione tramite S-box.

Funzione di sostituzione

Le S-box trasformano 6 bit in input in 4 bit di output, introducendo non-linearità cruciale per la sicurezza.

Permutazione finale

Ultima riorganizzazione che inverte la permutazione iniziale, completando il processo di cifratura.



Firma digitale e integrità dei dati



Integrità

Verifica che i dati non siano stati alterati durante la trasmissione o memorizzazione.



Autenticità

Conferma dell'identità del mittente attraverso la firma con chiave privata.



Non ripudio

Impossibilità di negare l'invio di un messaggio firmato digitalmente.

Esempi pratici hanno incluso **firme elettroniche e blockchain**, evidenziando le connessioni dirette con applicazioni reali del mondo digitale contemporaneo.

Funzioni hash crittografiche

Gli studenti hanno esplorato le proprietà fondamentali delle **funzioni hash**:

- **Deterministica**: stesso input → stesso output
- **Efficiente**: calcolo rapido del digest
- **Resistenza alle collisioni**: difficoltà di trovare due input con stesso hash
- **Effetto valanga**: piccole modifiche → grandi cambiamenti nell'output

Implementazioni pratiche con Python

Per consolidare la comprensione degli algoritmi crittografici, il laboratorio CriptoLab ha integrato **attività implementative in Python**, realizzate in ambiente Google Colab, rendendo tangibili i meccanismi interni della crittografia.

Cifrario di Cesare

Realizzazione di funzioni per cifratura/decifratura basate su traslazione e implementazione di un attacco a forza bruta.

Cifrario di Vernam

Funzione di conversione in ASCII binario, generazione di chiave casuale e cifratura/decifratura tramite XOR.

Data Encryption Standard

Implementazione della struttura a blocchi, chiavi simmetriche, permutazioni e sostituzioni, come modello della crittografia moderna.

Firma Digitale

Sviluppo di funzioni per la generazione del digest con hash, concatenazione per simulare la trasmissione firmata e verifica.

Questo approccio ha rafforzato le competenze computazionali e crittografiche degli studenti, promuovendo l'**autonomia** nella progettazione e codifica di algoritmi.

L'uso di Python in ambiente Google Colab ha abbassato la soglia di accesso, facilitando l'**apprendimento collaborativo** e l'**interazione** continua.

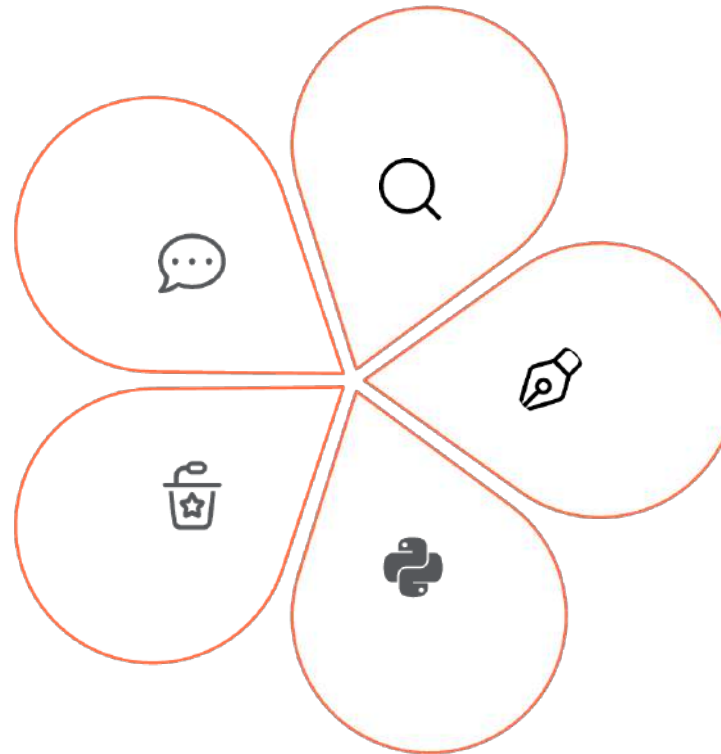
Metodologie didattiche innovative

Lezioni dialogate

Introduzione partecipativa dei concetti teorici attraverso domande stimolo e discussioni guidate.

Riflessione metacognitiva

Momenti strutturati di analisi del processo di apprendimento e delle competenze acquisite.



Cooperative learning

Apprendimento cooperativo per favorire l'interdipendenza e il peer tutoring tra studenti.

Esercitazioni manuali

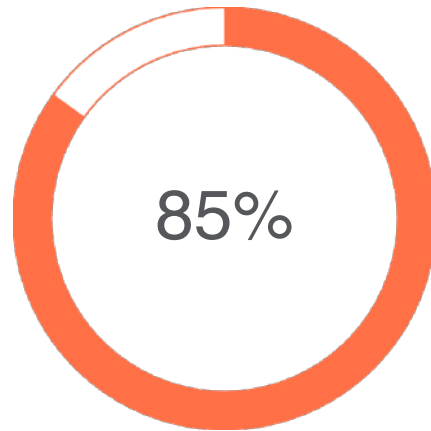
Attività pratiche di cifratura e decifratura per comprendere i meccanismi.

Coding in Python

Implementazione su Google Colab per tradurre immediatamente teoria in codice.

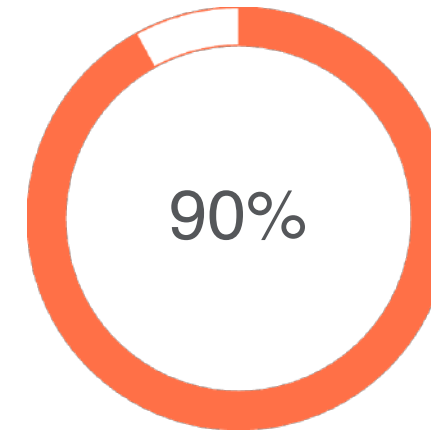
Risultati dell'esperienza formativa

L'impatto educativo del laboratorio ha prodotto **risultati significativi e misurabili** sulle competenze e la motivazione degli studenti partecipanti.



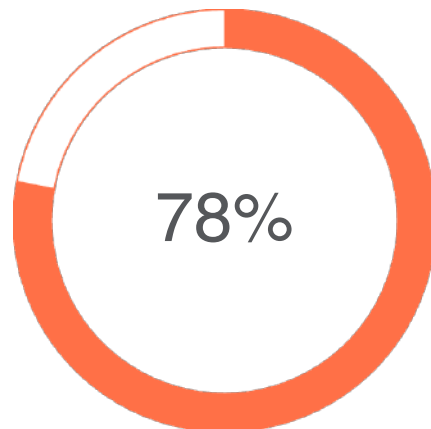
Autonomia progettuale

Studenti che hanno mostrato maggiore sicurezza nella progettazione indipendente di algoritmi



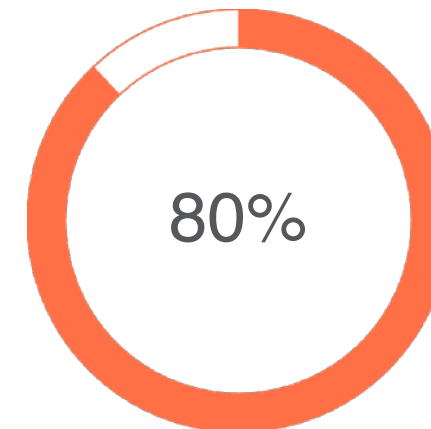
Teoria-pratica

Miglioramento nella capacità di tradurre concetti teorici in implementazioni pratiche



Problem solving

Sviluppo di competenze collaborative e di risoluzione creativa dei problemi



Interesse STEM

Crescita significativa della motivazione verso informatica scientifica e discipline STEM

Conclusioni e prospettive future

CriptoLab ha dimostrato come la **crittografia** possa rappresentare un potente catalizzatore didattico, capace di integrare armoniosamente matematica, informatica e consapevolezza sociale digitale.

Replicabilità

Il modello didattico è documentato e trasferibile in altri contesti educativi con materiali open source.

Scalabilità

L'esperienza può essere adattata a diversi livelli di istruzione e ampliata con moduli aggiuntivi specialistici.

Impatto didattico

Ha reso la didattica dell'informatica più coinvolgente, scientificamente rigorosa e professionalmente orientativa.

L'esperienza **CriptoLab** rappresenta un modello efficace per l'insegnamento dell'informatica, dimostrando come l'integrazione di teoria, pratica e riflessione critica possa trasformare l'apprendimento delle competenze digitali del futuro.



CriptoLab: alla scoperta della crittografia.

*Dalla teoria degli algoritmi al
coding crittografico*

Un'esperienza didattica innovativa per l'apprendimento
attivo degli **algoritmi crittografici**.

A cura di **Francesco Paolo Caforio**

Docente A-41 presso **I.I.S.S. "E. Majorana"** Martina Franca (TA)