# POLYLAB

## EECE 455 Project


**Presented by:**

Roaa Hajj Chehade
Ghada Al Danab
Aya El Hajj
Joud Senan

# OUTLINE

- Introduction
- Purpose
- Features
- Users' Journey
- Technologies Used
- Architecture Overview
- Calculator Testing
- Conclusion
- Demo

# Introduction

This project implements a GF($2^m$) polynomial arithmetic calculator for $2 \le m \le 8$, supporting:

- Addition & subtraction (XOR)
- Multiplication with modular reduction
- Division using multiplicative inverse
- Inversion via the Extended Euclidean Algorithm
- Exponentiation
- Hexadecimal input
- Full support for Binary, Hexadecimal, and Decimal output

# Purpose of the Project

**The Platform Aims To:**

- Provide a secure, role-based system for students, instructors, & admins
- Manage classrooms, assignments, submissions, and learning content
- Enforce strong security:
  - MFA
  - CSRF protection
  - Safe sessions
  - Hardened headers
- Offer a high-assurance GF($2^m$) calculator for cryptography coursework

# Why This Project Matters

- GF(2ᵐ) arithmetic is core to cryptography (AES, ECC, error correction)
- Students struggle to visualize finite-field operations
- Existing tools are either too technical or lack step-by-step clarity
- Our platform solves this with:
  - Intuitive interface
  - Validated operations
  - Clear polynomial-level visualization in one place

# Features

01

## Authentication

Secure signup, login, and email verification processes.

02

## User Roles

Defined roles for students, instructors, and admins.

03

## Classroom Management

Create and manage classrooms, assignments, and grading.

04

## Admin Panel

Review instructor requests and manage user roles effectively.

05

## GF(2^m) Calculator

Perform arithmetic operations on polynomials in GF(2^m).

06

## Security Features

Multi-factor authentication and strong security headers ensure safety.

## Students can

- join classrooms,
- view materials,
- submit assignments, use the calculator.

## Instructors can

- create classrooms,
- post assignments/material,
- grade and review submissions.

## Admin can

- approve instructors,
- manage roles,
- oversee platform.

# Technologies Used

## Frontend

- React 18, TypeScript
- Vite
- TailwindCSS

## Backend

- FastAPI, SQLAlchemy, Pydantic v2
- Argon2 password hashing
- pyotp (TOTP MFA)
- SQLite (default), Uvicorn

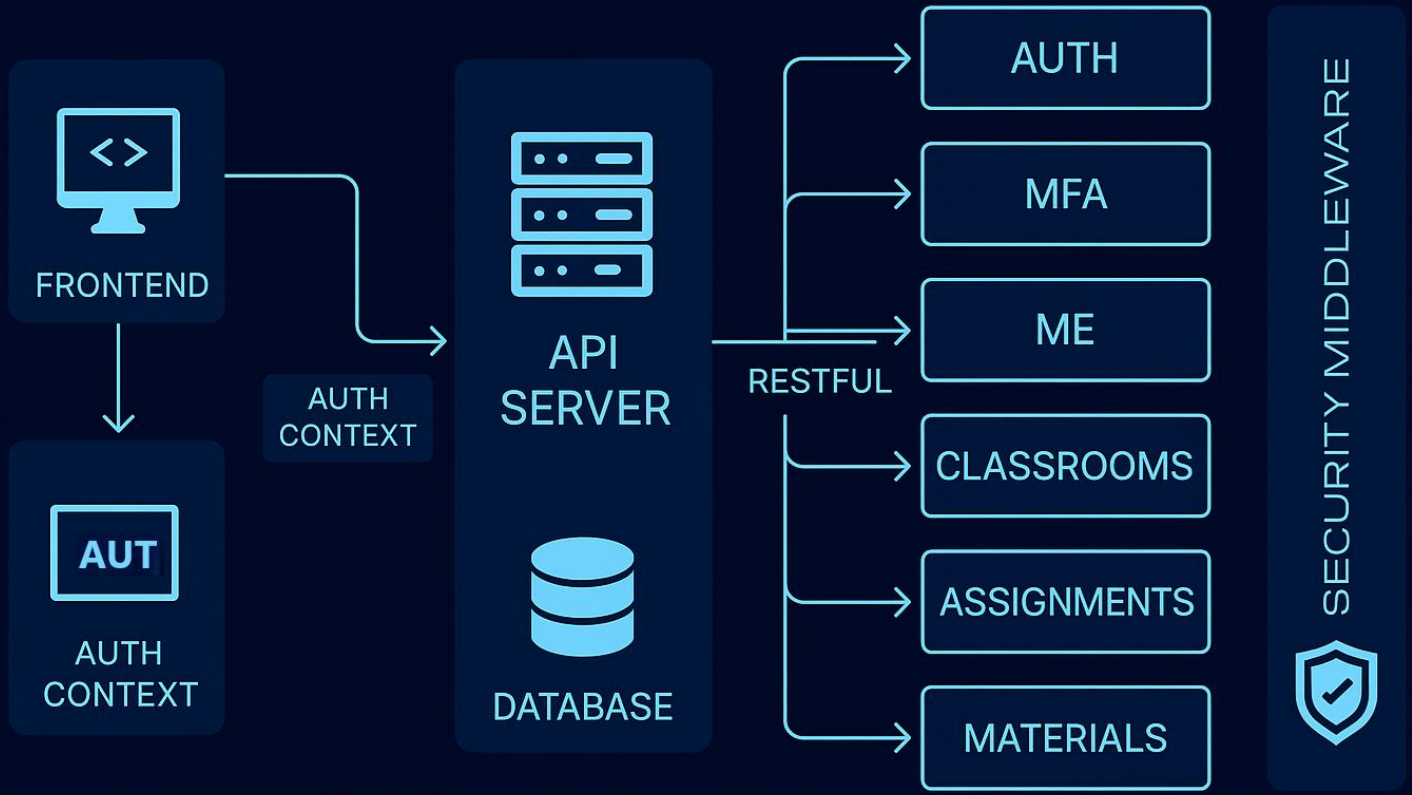
## Security

- HttpOnly cookies
- SameSite=Lax
- CSRF double-submit protection
- Rate limiting
- Security headers (CSP, XFO, XCTO, Referrer-Policy)
- Optional HSTS
- MFA (TOTP)

## Tools & Libraries

- JWT tokens for email verification
- OpenAPI/Swagger, File uploads

# ARCHITECTURE OVERVIEW



# GF($2^m$) Calculator Testing & Verification

01

## Exhaustive Brute-Force Testing (m = 2…8)

- Tested *every* element a and b in GF($2^m$)
- Verified:
  - ✓ Addition (XOR)
  - ✓ Multiplication
  - ✓ Modular reduction
  - ✓ Inversion
  - ✓ Exponentiation
- Total: **tens of thousands of test cases per field**

02

## Independent "Oracle" Implementation

- A second slow but mathematically simple model used to verify correctness:
  - ✓ Bitwise polynomial multiplication
  - ✓ Polynomial long-division
  - ✓ Brute-force inverse search
  - ✓ Naïve exponentiation

All outputs matched perfectly with our optimized implementation.

# GF(2ᵐ) Calculator Testing & Verification

## 03 Algebraic Identity Validation

- Checked fundamental field identities:
- $a+a=0$
- $a \cdot a^{-1}=1$
- $a^{2^m-1}=1$ (nonzero a)
- Neutral elements:
  - $a+0=a$
  - $a \cdot 1=a$

## 04 AES Gold Standards (GF(256))

- Verified well-known AES operations:
- $57 \times 13=FE$
- $57^2=A5$
- inv(57)=CA and $57 \cdot CA=1$

We built a tool where mathematics, security, and learning meet.
Because “When cryptography becomes visual, understanding becomes possible.”

# conclusion

- The system is a complete, secure, role-based educational platform
- Built with modern frontend and backend technologies
- Implements security best practices
- Includes a mathematically guaranteed accurate GF($2^m$) calculator
- Demonstrates strong architectural design, correctness, and reliability

# DEMO TIME!

# Thank you

# for listening !