[CS309] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Kunj Thakkar (202251142)

Autumn 2024-2025
Lecture (Week 5)

1 Foundations of Polynomial and Field Theory

The bedrock of modern cryptography lies in finite fields. To grasp these concepts fully, one must delve into the fundamentals of polynomials and field theory.

1.1 Irreducible Polynomials

Definition 1 *A polynomial $P(x) \in F[x]$ of degree $n \neq 1$ is deemed irreducible if it cannot be factored into a product of two non-constant polynomials in $F[x]$.*

For a polynomial $P(x)$ of degree > 1:

$$P(x) = P(x_1) \cdot P(x_2) \implies \text{at least one of } P(x_1) \text{ or } P(x_2) \text{ must be constant}$$

Example: $P(x) = x^2 + 1$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$ as $x^2 + 1 = (x + i)(x - i)$.

Irreducible polynomials are crucial in constructing finite fields, also known as Galois fields. For instance, $\mathbb{F}_{2^n}$ can be constructed using an irreducible polynomial of degree n over $\mathbb{F}_2$.

- $I = (P(x)) = \{q(x)P(x) \mid q(x) \in \mathbb{F}[x]\}$ defines an ideal in $\mathbb{F}[x]$.
- The quotient $\mathbb{F}[x]/(P(x))$ forms a field if $P(x)$ is irreducible.

1.2 Polynomial Operations

1.2.1 Multiplication

For polynomials $P_1(x)$ and $P_2(x)$:

$$\begin{aligned} P_1(x) &= a_0 + a_1x + a_2x^2 + \cdots \\ P_2(x) &= b_0 + b_1x + b_2x^2 + \cdots \\ P_1(x) \cdot P_2(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots \end{aligned}$$

1.2.2 Division

For polynomial $q(x)$ in $F[x]$:

$$q(x) = d(x)P(x) + r(x)$$

where $\deg(r(x)) < \deg(P(x))$. This forms the foundation for division within polynomial rings and is essential for algorithms like the Euclidean algorithm.

1.3 Field Examples

1.3.1 $\mathbb{R}[x]$

Consider $x^2 + 1$ in $\mathbb{R}[x]$. It's irreducible over $\mathbb{R}$ but factors in $\mathbb{C}[x]$:

$$x^2 + 1 = (x + i)(x - i)$$

1.3.2 $\mathbb{F}_2[x]$

In $\mathbb{F}_2 = \{0, 1\}$, $x^2 + x + 1$ is irreducible. It generates a field extension of $\mathbb{F}_2$:

$$\mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$$

In this field, $x^2 = x + 1$.

2 Advanced Encryption Standard (AES)

AES, introduced by NIST in 2001, is a symmetric encryption algorithm based on the Rijndael cipher. It operates as an iterated block cipher, encrypting data in fixed-size blocks through multiple rounds.

2.1 AES Variants

Variant	Block Size	Rounds	Key Size
AES-128	128 bits	10	128 bits
AES-192	128 bits	12	192 bits
AES-256	128 bits	14	256 bits

2.2 AES Round Structure

- First 9 rounds: SubBytes, ShiftRows, MixColumns
- 10th round: SubBytes, ShiftRows (no MixColumns)

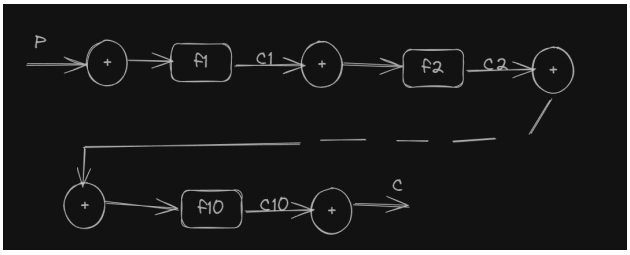

Figure 1: AES Round Structure

2.3 SubBytes Operation

SubBytes is a non-linear substitution step using an S-box:

$$S(x) = y, \quad \text{where } y \text{ is an 8-bit output}$$

For $x = \langle C_7, C_6, C_5, C_4, C_3, C_2, C_1, C_0 \rangle$:

$$S(C_7C_6C_5C_4C_3C_2C_1C_0) = \text{8-bit output}$$

2.4 Key Expansion

AES uses a key schedule to derive round keys:

- RotWord: Cyclic permutation of word bytes
- SubWord: S-box substitution for each byte
- Rcon: Addition of round constant

2.5 MixColumns Operation

MixColumns provides diffusion in AES:

- Each state column is treated as a polynomial over F_{2^8}
- Multiplied by fixed polynomial $c(x) = 03x^3 + 01x^2 + 01x + 02$
- Multiplication modulo $x^4 + 1$

This operation ensures that small input changes affect many output bits, enhancing AES's security.