The University of Sydney
School of Computer Science
Dr Suranga Seneviratne
Senior Lecturer - Security

THE UNIVERSITY OF SYDNEY

Abstract Algebra

This handout covers the concepts of Abstract Algebra that you will need to understand the inner workings of cryptography.

1 Algebraic Structures

Abstract algebra is a branch of mathematics that studies algebraic structures such as groups, rings, fields, and modules. These structures form the foundations for mathematical concepts beyond basic arithmetic and geometry. In cryptography, abstract algebra is crucial because it underpins the structure and security of many encryption algorithms and systems, providing the mathematical basis for constructing and analyzing cryptographic protocols.

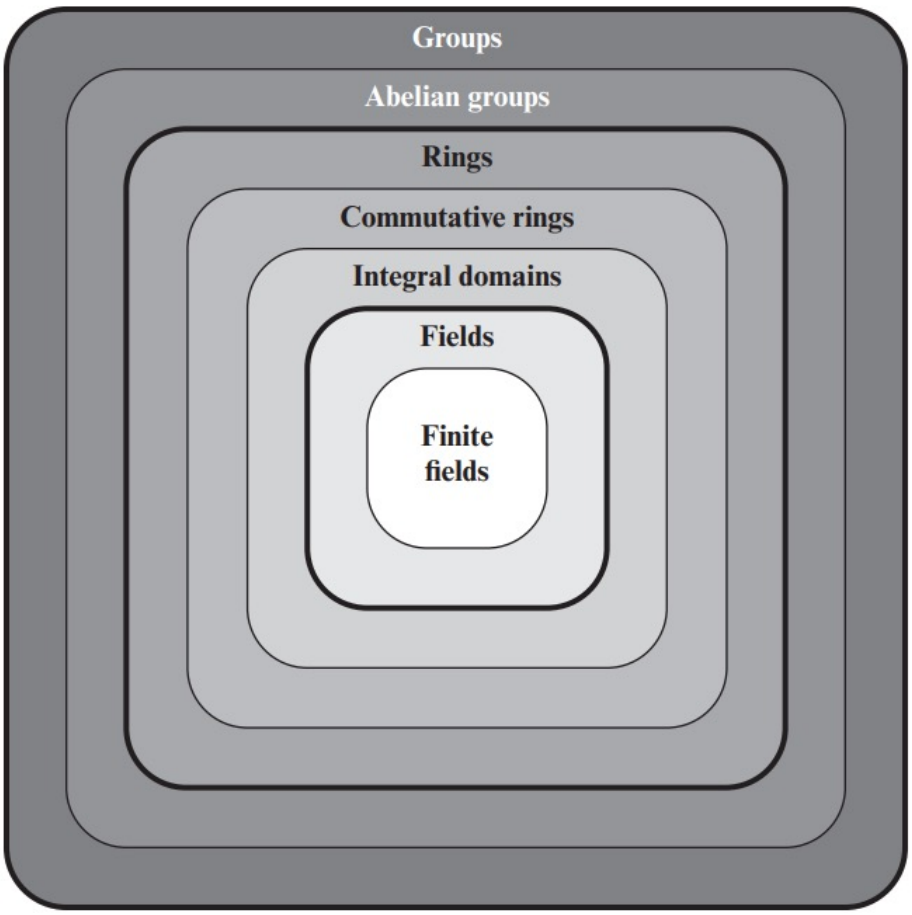

Figure 1: Bird's eye view of how common algebraic structures are related

*__Source:__ Cryptography and Network Security – 7th Edition by William Stallings

- **Set:** The foundation, a collection of elements without any defined algebraic operations.

- **Group:** A set with an associative binary operation, satisfying closure, the existence of an identity element, and the existence of inverses. A special kind of group is the Abelian Group.
- **Abelian (Commutative) Group:** A group with a commutative binary operation.
- **Ring:** A set with two binary operations (addition and multiplication) that is an Abelian group under addition, closed under multiplication, associative under multiplication, and satisfies distributivity of multiplication over addition. Rings can be specialized further.
- **Commutative Ring:** A ring where multiplication is commutative.
- **Ring with Unity (Unital Ring):** A ring with a multiplicative identity.
- **Integral Domain:** A commutative ring with unity that has no zero divisors (if $a.b = 0$ then $a = 0$ or $b = 0$).
- **Field:** A commutative ring with unity where every non-zero element has a multiplicative inverse, supporting addition, subtraction, multiplication, and division (except by zero). A special type of a field is the finite field
- **Finite Field (Galois Field):** A field with a finite number of elements. Finite fields play crucial roles in number theory, cryptography, and coding theory.

2 Groups

A **group** is an algebraic structure consisting of a set, G, together with an operation $+$ (referred to as "addition") that combines any two elements a and b from G to form another element in G. The operation and the set must satisfy four fundamental properties:

1. **Closure**: For all $a, b \in G$, the result of the operation $a + b$ is also in G.
2. **Associativity**: For all $a, b, c \in G$, the equation $(a + b) + c = a + (b + c)$ holds.
3. **Identity Element**: There exists an element 0 in G, known as the "zero element" or "additive identity," such that for any element a in G, the equation $0 + a = a + 0 = a$ holds.
4. **Inverse Elements**: For each element a in G, there exists an element $-a$ in G such that $a + (-a) = (-a) + a = 0$, where 0 is the additive identity of the group.

When the operation $+$ is commutative, meaning $a + b = b + a$ for all $a, b \in G$, the group is referred to as an **abelian group** or **commutative group**. In the context of addition, groups are inherently abelian, as addition is typically a commutative operation. Also, note that the definition of groups is about having a binary operation (Section 1) - it doesn't have to be addition. It can also be multiplication.

3 Abelian Groups

An **Abelian group**, also known as a **commutative group**, is a group $(G, +)$ in which the group operation $+$ is commutative. This means that for all elements a and b in G, the equation $a + b = b + a$ holds. In other words, the order in which two elements are combined using the group operation does not affect the outcome.
Formally, an Abelian group satisfies the following properties:

1. **Closure**: For all $a, b \in G$, the result of the operation $a + b$ is also in G.
2. **Associativity**: For all $a, b, c \in G$, the equation $(a + b) + c = a + (b + c)$ holds.
3. **Identity Element**: There exists an element 0 in G, known as the additive identity, such that for any element a in G, the equation $0 + a = a + 0 = a$ holds.
4. **Inverse Elements**: For each element a in G, there exists an element $-a$ in G such that $a + (-a) = (-a) + a = 0$, where 0 is the additive identity of the group.
5. **Commutativity**: For all $a, b \in G$, $a + b = b + a$.

The addition operation $+$ is often used in the context of Abelian groups, but the group operation can be any binary operation that satisfies these properties. The notation and specific operation might vary depending on the context and the elements of the set G.

Example: The set of integers $\mathbb{Z}$ is an Abelian group under addition.
To prove that the set of integers $\mathbb{Z}$ forms an Abelian group under addition, we need to verify the following group properties:

1. **Closure**: For any two integers $a, b \in \mathbb{Z}$, their sum $a + b$ is also an integer, implying that $\mathbb{Z}$ is closed under addition. *Example*: $3, 5 \in \mathbb{Z}$ and $3 + 5 = 8 \in \mathbb{Z}$.
2. **Associativity**: For any three integers $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$. *Example*: Let $a = 2, b = 3, c = 4$. Then $(2 + 3) + 4 = 5 + 4 = 9$ and $2 + (3 + 4) = 2 + 7 = 9$.
3. **Identity Element**: The integer 0 acts as the identity element for addition because for any integer $a \in \mathbb{Z}$, $a + 0 = a$ and $0 + a = a$. *Example*: For $a = 7$, $7 + 0 = 7$ and $0 + 7 = 7$.
4. **Inverses**: For every integer $a \in \mathbb{Z}$, there exists an inverse $-a \in \mathbb{Z}$ such that $a + (-a) = 0$. *Example*: For $a = 5$, the inverse is -5 since $5 + (-5) = 0$.
5. **Commutativity**: The sum of any two integers $a, b \in \mathbb{Z}$ is commutative, meaning $a + b = b + a$. *Example*: Let $a = 4, b = 6$. Then $4 + 6 = 10$ and $6 + 4 = 10$.

By verifying these properties, we conclude that the set of integers $\mathbb{Z}$ under the operation of addition forms an Abelian group.

4 Rings

A **ring** is a mathematical structure that consists of a set equipped with two binary operations: addition and multiplication following the below properties:

1. **Closure**: For any two elements a and b in the set, both $a + b$ and $a \cdot b$ are also in the set.
2. **Associativity**: For all elements a, b, and c in the set, the equations $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ hold.
3. **Additive Identity**: There exists an element 0 in the set such that for any element a in the set, $a + 0 = a$.
4. **Additive Inverse**: For every element a in the set, there exists an element $-a$ in the set such that $a + (-a) = 0$.
5. **Commutativity of Addition**: For all elements a and b in the set, $a + b = b + a$.
6. **Distributive Laws**: For all elements a, b, and c in the set, the equations $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ hold.

Note that multiplication in a ring does not necessarily have to be commutative (i.e., $a \cdot b = b \cdot a$ might not always hold), and there might not be a multiplicative identity element (an element 1 such that $a \cdot 1 = a$ for any a in the set). If a ring does have a multiplicative identity and multiplication is commutative, it is called a **commutative ring**. If every nonzero element of a commutative ring has a multiplicative inverse, the structure is known as a **field**.

Example: Similar to the above example you can show that set of integers $\mathbb{Z}$ is a ring.

5 Commutative Rings

In addition to the above properties of the rings, commutative rings are commutative under multiplication.

7. **Commutativity of Multiplication**: For all elements a and b in the set, $a.b = b.a$.

Example: Note that the set of integers $\mathbb{Z}$ is also a commutative ring.

6 Fields

Fields satisfy the existence of a multiplicative inverse in addition to all the properties of a commutative ring.

1. **Closure**: For any two elements a and b in the set, both $a + b$ and $a \cdot b$ are also in the set.
2. **Associativity**: For all elements a, b, and c in the set, the equations $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ hold.
3. **Additive Identity**: There exists an element 0 in the set such that for any element a in the set, $a + 0 = a$.
4. **Additive Inverse**: For every element a in the set, there exists an element $-a$ in the set such that $a + (-a) = 0$.

5. **Commutativity of Addition**: For all elements a and b in the set, $a + b = b + a$.
6. **Distributive Laws**: For all elements a, b, and c in the set, the equations $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ hold.
7. **Commutativity of Multiplication**: For all elements a and b in the set, $a.b = b.a$.
8. **Multiplicative Inverse**: For every element a in the set except for 0, there exists an element a^{-1} in the set such that $a.a^{-1} = 1$.

Example: Show the set of integers $\mathbb{Z}$ is not a Field.

Here, we can show that by providing a counter-example related to the existence of multiplicative inverse.

For example, if we consider 4 its multiplicative identify is $\frac{1}{4}$, i.e., $4.\frac{1}{4} = 1$. However $\frac{1}{4} \notin \mathbb{Z}$. Therefore, the elements of $\mathbb{Z}$ do not have multiplicative inverses and as a result, $\mathbb{Z}$ is not a Field.

Example: On the other hand, the set of rational numbers $\mathbb{Q}$ is a Field.

For example, if we consider 4 its multiplicative identify is $\frac{1}{4}$, i.e., $4.\frac{1}{4} = 1$. Now, $\frac{1}{4} \in \mathbb{Q}$. Therefore, the elements of $\mathbb{Q}$ have multiplicative inverses and as a result, $\mathbb{Q}$ is a Field.

7 Finite Fields (Galois Fields)

A field with a finite number of elements is called a Finite Field. They are also called as Galois fields and come in two primary types based on their size.

1. **Prime fields**: A prime field is a finite field with p elements, where p is a prime number. The prime field of order p is denoted as $\mathbb{F}_p$ or GF(p). Its elements can be thought of as the set of integers $\{0, 1, 2, ..., p-1\}$ with addition and multiplication performed modulo p. The prime field has a characteristic of p, meaning that p is the smallest positive integer such that the sum of p copies of any element is 0.
2. **Extension fields**: Extension fields are finite fields with p^n elements, where p is a prime number and n is a positive integer greater than 1. These fields are denoted as $\mathbb{F}_{p^n}$ or GF(p^n). They can be constructed as extensions of a prime field $\mathbb{F}_p$ by adding elements that are roots of irreducible polynomials of degree n over $\mathbb{F}_p$. Essentially, you're creating a field that contains all the elements of the prime field along with the roots of these polynomials and all possible sums, products, and multiples of these roots and the elements of the prime field. **In this unit we will not go into the details of how to find the irreducible polynomial and and the elements of** $GF(p^n)$.

Example: Using examples demonstrate that $\mathbb{F}_7$ is a field.

$\mathbb{F}_7$ is calls called as the $GF(7)$ and the elements of it as $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$

1. **Closure**: For any two elements a and b in the set, both $a + b$ and $a \cdot b$ are also in the set.

   E.g. 5 and 6 $\in \mathbb{F}_7$.

   Addition - $5 + 6 \mod 7 = 4$ and $4 \in \mathrm{F}_7$.
   Multiplication$-5{\cdot}6 \mod 7 = 2$ and $2 \in \mathrm{F}_7$.

2. **Associativity**: For all elements a, b, and c in the set, the equations $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ hold.

   E.g. 1,, 4, 5, and 6 $\in \mathbb{F}_7$.

   Addition - $(5+6)+4 \mod 7 = 1$ and $5+(6+4) \mod 7 = 1 \implies 5+6)+4 = 5+(6+4)$
   Multiplication - $(5.6)4 \mod 7 = 1$ and $5(6.4) \mod 7 = 1 \implies (5.6)4 = 5(6.4)$.

3. **Additive Identity**: There exists an element 0 in the set such that for any element a in the set, $a + 0 = a$.

   E.g. 0, and 5 $\in \mathbb{F}_7$.

   $5 + 0 \mod 7 = 5$ i.e., there exists 0 which is the additive identity.

4. **Additive Inverse**: For every element a in the set, there exists an element $-a$ in the set such that $a + (-a) = 0$.

   E.g. 0, 2 and 5 $\in \mathbb{F}_7$.

   $5 + 2 \mod 7 = 0$ i.e., 2 is the additive inverse of 5.

   Another example, $4 + 3 \mod 7 = 0$ i.e., 3 is the additive inverse of 4.

5. **Commutativity of Addition**: For all elements a and b in the set, $a + b = b + a$.

   E.g. 0, 2 and 5 $\in \mathbb{F}_7$.

   $5 + 2 \mod 7 = 0$ and $2 + 5 \mod 7 = \implies 5 + 2 = 2 + 5$.

6. **Distributive Laws**: For all elements a, b, and c in the set, the equations $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ hold.

   E.g. 0, 2, 4 and 5 $\in \mathbb{F}_7$.

   $5(2 + 4) \mod 7 = 2$ and $5.2 + 5.4 \mod 7 = 2 \implies 5(2 + 4) = 5.2 + 5.4$. Similarly, $(a + b) \cdot c = a \cdot c + b \cdot c$ can be demonstrated as well.

7. **Commutativity of Multiplication**: For all elements a and b in the set, $a.b = b.a$.

   E.g. 2, 3, 5 and 5 $\in \mathbb{F}_7$.

   $5.2 \mod 7 = 3$ and $2.5 \mod 7 = 3 \implies 5.2 = 2.5$.

8. **Multiplicative Inverse**: For every element a in the set except for 0, there exists an element a^{-1} in the set such that $a.a^{-1} = 1$.

   $5.3 \mod 7 = 1 \implies 3$ is the multiplicative inverse of 5. Note here both 3 and 5 $\in \mathbb{F}_7$.

   $6.6 \mod 7 = 1 \implies 6$ is the multiplicative inverse of 6. You can find this by iterating through all the elements of $\mathbb{F}_7$ or by using the extended Euclidean algorithm we discussed earlier.

Note: $\mathbb{F}_p$ is a finite filed only when p is a prime.

The generic case we denote this set is $Z_n = \{0, 1, 2, ..., n-1\}$ and it is only a commutative ring under modulo n. Normally this is denoted by $\mathbb{Z}/n\mathbb{Z}$.

For example let's take the case of $n = 8$, therefor $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is a commutative ring under modulo 8 because 8 is not a prime. While we have to show all the properties of a commutative ring to fully show this, here we give a counter example of a case where the multiplicative inverse does not exist - i.e., show that $\mathbb{Z}_n$ is not a finite field.

Lets consider $2 \in \mathbb{Z}_n$. Now if there is a multiplicative inverse $a \in \mathbb{Z}_n$ for 2 it must satisfy the equations that $2.a \mod 8 \equiv 1$.

Since 2 and 8 share a common factor, $2.b$ will never leave a remainder of 1 when divided by 8.

Let's iterate through the elements of $\mathbb{Z}_n$ and see whether this is true.

$2.0 \mod 8 = 0$
$2.1 \mod 8 = 2$
$2.2 \mod 8 = 0$
$2.3 \mod 8 = 6$
$2.4 \mod 8 = 0$
$2.5 \mod 8 = 2$
$2.6 \mod 8 = 4$
$2.7 \mod 8 = 6$

Note none of the calculations result in 1.

This also shows that for the extension fields $GF(2^n)$ (or $\mathbb{F}_{p^n}$) to work as finite filed we have to define something more. What we actually demonstrated is that under normal terms $GF(2^3)$ is not a finite field, but a commutative ring. Therefore we need polynomial arithmetic with modulo irreducible polynomials.

8 Polynomial Arithmetic with Modulo Irreducible Polynomial

Polynomial arithmetic modulo, an irreducible polynomial, is a foundational concept in the construction of finite fields, particularly extension fields. The key ideas are as follows.

- **Polynomial Arithmetic:** Just like arithmetic with numbers, you can add, subtract, multiply, and divide polynomials. For example, if you have two polynomials $p(x) = x^2 + 1$ and $q(x) = x + 2$ you can add them together to get $r(x) = x^2 + x + 3$.
- **Modulo Operation:** In the context of polynomials, the modulo operation involves dividing one polynomial by another and taking the remainder as the result. This is akin to how we take the remainder in integer modulo arithmetic but applied to polynomial division.

- **Irreducible Polynomial:** A polynomial is irreducible over a given field if it cannot be factored into polynomials of lower degree with coefficients in that field. For example, x^2+1 is irreducible over the real numbers (as it cannot be factored into real polynomials of lower degree) but not over the complex numbers (since it can be factored as $(x+i)(x-i)$.

When we say "Polynomial Arithmetic with Modulo Irreducible Polynomial," we refer to performing polynomial arithmetic operations where, upon multiplication or division, we take the result modulo an irreducible polynomial. This operation ensures that the outcomes always remain within a certain set of polynomials of a degree less than that of the irreducible polynomial, thereby facilitating the creation of a finite field.

8.1 Formation of $GF(2^3)$

Let's try to simplify the formation of $GF(2^3)$ as an example.

1. **Base Fields -** Start with $GF(2)$, which is the simplest finite field consisting of two elements: 0 and 1. Here, addition and multiplication are performed modulo 2.
2. **Choose an Irreducible Polynomial -** To construct $GF(2^3)$, we need an irreducible polynomial of degree 3 over $GF(2)$. An example is $p(x) = x^3 + x + 1$. This polynomial cannot be factored into polynomials of lower degree with coefficients in $GF(2)$.
3. **Define Elements -** Based on the power of 2, we know that the field will have 8 elements and 0 and 1 are already elements. The full list of elements are; $0, 1, x, x^2, x+1, x^2+1, x^2+x, x^2+x+1$. These elements can also be written as binary codes.

   $000 = 0$
   $001 = 1$
   $010 = x$
   $011 = x + 1$
   $100 = x^2$
   $101 = x^2 + 1$
   $110 = x^2 + x$
   $111 = x^2 + x + 1$
4. **Define the Operations -** Arithmetic operations within this field (addition, multiplication) must be performed modulo 2, and, for multiplication, modulo the base polynomial $p(x) = x^3 + x + 1$.

   Example addition Adding $x^2 + x$ and $x + 1$ is

   $x^2 + x + x + 1 = x^2 + 0x + 1 = x^2 + 1$ since $x + x = 0 \mod 2$

   Example multiplication Multiplying x and $x + 1$ is

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

   Example multiplication Multiplying x^2 and $x + 1$ is

   $x^2(x + 1) = x^3 + x^2$ here, the degree of the polynomial is greater than two. So we have to reduce it using $p(x) = x^3 + x + 1$.

   That is we need to find the remainder of $\frac{x^3+x^2}{x^3+x+1}$.

   Here we use an important idea. That is in modulo 2 arithmetic, 1+1=0, and similarly, 11=0 meaning the concept of "subtracting" is equivalent to adding because there are

no negative numbers; you're effectively flipping bits (0 to 1, or 1 to 0) when you "subtract".

We can write the remainder of our division as $x^3+x^2-(x^3+x+1) = x^2-x-1 = x^2+x+1$

8.2 Formation of $GF(2^8)$

$GF(2^8)$ is one of the most important finite fields in cryptography. There are several reasons why it is chosen as the fundamental field in important cryptographic schemes such as AES (Advanced Encryption Standards). Those reasons include $GF(2^8)$;

1. Striking a balance between computational efficiency and security - large enough to provide a good level of security for various cryptographic applications while still being small enough for efficient implementation in both hardware and software.
2. The binary nature of $GF(2^8)$ (being a field of 2^8 elements) aligns well with digital systems, which inherently process binary data.

Elements in $GF(2^8)$ can be represented as polynomials of degree less than 8, with coefficients in GF(2), which means each coefficient can either be 0 or 1. A general element in $GF(2^8)$ can be represented as:

$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ where $a_i \in \{0, 1\}$ for $i = 0, 1, \ldots, 7$. A commonly used irreducible polynomial in $GF(2^8)$ is $x^8 + x^4 + x^3 + x + 1$.

8.2.1 Addition in GF(2^8)

Addition (and Subtraction): In $GF(2^8)$, addition and subtraction are performed using the XOR operation, due to the binary nature of the field. This operation aligns with the principle that $1 + 1 = 0$ in binary arithmetic, which mirrors the XOR truth table.

Example: Consider adding two elements $a = x^6+x^4+x^2$ and $b = x^7+x^4+x^3+x$, represented in binary as $a = 01010100$ and $b = 10011010$. The sum $c = a + b$ is found by XORing a and b:

$c = 01010100 \oplus 10011010 = 11001110$,

which translates back to $x^7 + x^6 + x^3 + x^2 + x^1$.

8.2.2 Multiplication in $GF(2^8)$

Multiplication in $GF(2^8)$ involves a combination of shifting (to simulate multiplication by (x) and conditional XOR (for modular reduction by an irreducible polynomial). In understanding cryptography, in particular AES what we need is multiplying by x.

Example Multiplying by x and Modular Reduction Example

Suppose we have $a = x^7 + x^6$, which we want to multiply by x and then reduce. In binary, a is represented as 11000000.

Step 1: Multiply a by x

- Multiplying a by x (shifting left by 1): $11000000 \cdot x = 110000000$.
- In binary, this shift results in a 9-bit string due to the overflow, representing a polynomial of degree 8, which is $x^8 + x^7$ or 110000000.

Step 2: Modular Reduction

- Since we now have a degree 8 polynomial, we need to reduce it modulo the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, or 100011011 in binary.
- Reduction involves XORing the result with a shifted version of the irreducible polynomial to ensure the result fits within 8 bits.

Let's break down the XOR operation for reduction:

- The 9-bit result from the multiplication is 110000000.
- We align the most significant bit of the irreducible polynomial (100011011) with the most significant bit of our result and perform XOR:
- $110000000 \oplus 100011011 = 010011011$.

Now, our result is back within 8 bits, represented as 10011011 in binary, corresponding to the polynomial $x^7 + x^4 + x^3 + x + 1$.

8.3 Groups, Rings, and Fields in Cryptography

8.3.1 Advanced Encryption Standard (AES)

AES - the current state-of-the-art symmetric encryption method, uses the arithmetic of $GF(2^8)$, primarily in its S-boxes for the SubBytes step of encryption. The S-boxes perform a substitution on each byte of the data being encrypted by mapping it to its multiplicative inverse in $GF(2^8)$, followed by an affine transformation. This use of $GF(2^8)$ ensures non-linearity and resistance against certain types of cryptanalysis, making AES a strong and secure encryption method.

8.3.2 RSA

RSA encryption, named after its inventors Rivest, Shamir, and Adleman, is a public-key cryptosystem (i.e., asymmetric encryption). In the context of RSA, the relevant ring is the set of integers modulo n (denoted $\mathbb{Z}_n$), where n is the product of two large prime numbers, p and q. This ring includes all integers from 0 to $n - 1$, with addition and multiplication defined modulo n.

8.3.3 Discrete Logarithm Problem (DLP)

The discrete logarithm problem (which we discussed under number theory) is usually defined within the context of cyclic groups. A cyclic group is a type of group that can be generated by repeatedly applying the group operation to a single element, known as a generator of the group.

Given a cyclic group G, generated by an element g, and another element h in G, the discrete logarithm problem asks for the integer x (if it exists) such that:

$$g^x = h$$

Here, g^x denotes applying the group multiplication operation to g with itself x times, and x is called the "logarithm" of h to the base g. Note that g indeed is the primitive root we discussed under number theory. DLP is key to many cryptographic schemes.

8.3.4 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an example of asymmetric cryptography that uses the properties of elliptic curves over finite fields. It relies on the difficulty of the elliptic curve discrete logarithm problem (ECDLP) for its security. ECC operates on the points of an elliptic curve, which form a group with well-defined addition operations. The efficiency and strength of ECC allow for smaller key sizes compared to RSA, for a comparable level of security. This makes ECC particularly appealing for use in environments with constrained resources. In this unit we do not go into the details of ECC.

8.3.5 Digital Signature Algorithm (DSA) and Elliptic Curve DSA (ECDSA)

DSA is a standard for digital signatures that operates within the framework of modular arithmetic and finite fields. It is based on the security of the discrete logarithm problem. Similarly, ECDSA is a variant that uses elliptic curve groups to provide the same functionality. Both DSA and ECDSA rely on the properties of groups to secure digital signatures, ensuring the authenticity and integrity of digital messages or documents.

8.3.6 Diffie-Hellman Key Exchange (DH) and Elliptic Curve Diffie-Hellman (ECDH)

The Diffie-Hellman Key Exchange algorithm is a method of securely exchanging cryptographic keys over a public channel. It is based on the difficulty of calculating discrete logarithms in a finite field. ECDH is an adaptation of DH that uses elliptic curve cryptography. Both of these protocols leverage the mathematical properties of groups to allow two parties to generate a shared secret key used for secure communication.

8.3.7 Cryptographic Hash Functions

While hash functions are not encryption in the traditional sense, they are a crucial aspect of cryptographic protocols, providing data integrity checks and playing a key role in the implementation of digital signatures and various authentication schemes. Some hash functions are designed using algebraic structures to achieve desired properties such as collision resistance and preimage resistance.