# Fields in Cryptography


Çetin Kaya Koç

http://cs.ucsb.edu/~koc

koc@cs.ucsb.edu


# Field Axioms

- A field $\mathcal{F}$ consists of a set $S$ and two operations which we will call addition and multiplication, and denote them by $\oplus$ and $\otimes$
- The set $S$ has two special elements, denoted by 0 and 1
- The set $S$ and the addition operation $\oplus$ form an additive group denoted by $G_a = (S, \oplus)$ such that 0 is the neutral (identity) element of $G_a$
- Also the set $S^* = S - \{0\}$ and the multiplication operation $\otimes$ form a multiplicative group denoted by $G_m = (S^*, \otimes)$ such that 1 is the neutral (identity) element of $G_m$
- Furthermore, the distributivity of multiplication over addition holds:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \quad \text{for} \quad a, b, c \in S$$

# Size and Characteristic

- The number of elements in a field is the **size** of the field, which can be finite or infinite
- The **characteristic** $k$ of a field is the smallest number of times one must use 1 (the identity element of $G_m$) in a sum (using the addition operation $\oplus$) to obtain 0 (the identity element of $G_a$)

$$\overbrace{1 \oplus 1 \oplus \cdots \oplus 1}^{k \text{ 1s}} = 0$$

- The characteristic is said to be zero, if the repeated sum never reaches the additive identity element 0

# Rings

- The set of integers $\mathcal{Z}$ and the integer addition $+$ and multiplication operation $\times$ does not form a field
- We can easily verify that $(\mathcal{Z}, +)$ is an additive group with identity 0
- However, $(\mathcal{Z} - \{0\}, \times)$ is not a multiplicative group; for example, the element $2 \in \mathcal{Z} - \{0\}$, however, it does not have an inverse: There is no such $x \in \mathcal{Z} - \{0\}$ that would give $2 \times x = 1$
- In fact, $(\mathcal{Z}, +, \times)$ forms a **ring**, another mathematical structure similar to field, which does not require a multiplicative group
- In a ring, the distributivity of multiplication over addition holds

# Infinite Fields

- A rational number is defined to be a number of the form $\frac{a}{b}$ such that $b \neq 0$ and $a, b \in \mathcal{Z}$
- The set of rational numbers $\mathcal{Q}$ together with the usual addition $+$ and multiplication $\times$ operations, with additive and multiplicative identities 0 and 1, respectively, forms a field
- Indeed, $(\mathcal{Q}, +)$ is an additive group with identity 0; the additive inverse of $\frac{a}{b}$ is found as $-\frac{a}{b}$
- Also, $(\mathcal{Q}, \times)$ is a multiplicative group with identity 1; the multiplicative inverse of $\frac{a}{b}$ with with $a \neq 0$ is found as $\frac{b}{a}$
- The size of the field $\mathcal{Q}$ is infinity; the characteristic of $\mathcal{Q}$ is zero since the sum $1 + 1 + \cdots + 1$ can never be equal to 0

# Infinite Fields

- Similarly, the set of real numbers $\mathcal{R}$ together with the usual addition $+$ and multiplication $\times$ operations, with additive and multiplicative identities 0 and 1, respectively, form a field
- Also, the set of complex numbers $\mathcal{C}$ together with the usual addition $+$ and multiplication $\times$ operations, with additive and multiplicative identities 0 and 1, respectively, forms a field
- Both of these fields have infinite size and zero characteristic
- In cryptography, we deal with computable objects, and we have finite memory, therefore, infinite fields are not suitable
- In cryptography, we deal with finite fields, a branch of mathematics where the name of Évariste Galois has a special place

# Évariste Galois

- Évariste Galois (1811-1832) was a French mathematician born in Bourg-la-Reine
- While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a long-standing problem
- His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra, and the subfield of Galois connections
- He was the first person to use the word “group” (French: groupe) as a technical term in mathematics to represent a group of permutations
- A radical Republican during the monarchy of Louis Philippe in France, he died from wounds suffered in a duel under questionable circumstances at the age of twenty

# Finite Fields

- First we observe that for a prime $p$ the set $\mathcal{Z}_p$ together with the addition and multiplication mod $p$ operations forms a finite field of $p$ elements: we will denote this field by GF($p$), the Galois field of $p$ elements
- The additive group $(\mathcal{Z}_p, +)$ has the elements $\mathcal{Z}_p = \{0, 1, 2, \ldots, p-1\}$, the operation is addition mod $p$, and the additive identity element is 0
- The multiplicative group $(\mathcal{Z}_p^*, \times)$ has the elements $\mathcal{Z}_p^* = \{1, 2, \ldots, p-1\}$, the operation is multiplication mod $p$, and the multiplicative identity element is 1
- The size of GF($p$) is $p$, while the characteristic is also $p$ since

$$\overbrace{1 + 1 + 1 + \cdots + 1}^{p \quad 1\text{s}} = 0$$

# The Smallest Field: GF(2)

- Since 2 is a prime, GF(2) is a Galois field of 2 elements
- The set is given as $\{0, 1\}$; the size is 2, and the characteristic is 2
- The additive identity is 0 while the multiplicative identity is 1
- The addition and multiplication operations are as follows:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\times$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

- In other words, the addition operation in GF(2) is equivalent to the Boolean exclusive OR operation, while the multiplication operation in GF(2) is the Boolean AND operation

# GF(3)

- 3 is also a prime, and thus, GF(3) is a Galois field of 3 elements
- The set is given as $\{0, 1, 2\}$; the size is 3, and the characteristic is 3
- The additive identity is 0 while the multiplicative identity is 1
  the additive group: $(\{0, 1, 2\}, +)$, the multiplicative group: $(\{1, 2\}, \times)$
- The addition and multiplication operations in GF(3) are defined as mod 3 addition and mod 3 multiplication, respectively:

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\times$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

# Finite Fields with Composite Number Size

- Since the size $p$ of GF($p$) is a prime, a question one can pose is whether there are fields of size other than a prime
- For example, is there a field with 6 elements?
- We can try to see if mod 6 arithmetic works, however, we already know that multiplicative inverse of certain elements mod 6 do not exist
- For example, 3 does not have a multiplicative inverse in mod 6, since there is no number $a$ that satisfies

$$3 \cdot a = a \cdot 3 = 1 \pmod{6}$$

- So, our question remains: Is there a field with 6 elements?

# Finite Fields of Size Prime Power

- Galois showed that the size of a finite field can only be a power of a prime number, in other words, $p^k$ for $k = 1, 2, 3, \ldots$
- There is a particular construction of such fields, in fact, we already know how to construct GF($p$), it is simply mod $p$ arithmetic over $\mathcal{Z}_p$
- How does one construct GF($p^2$) or GF($p^3$), etc.
- For example, what is the set and the arithmetic of GF($7^3$)?

# Construction of GF($2^k$)

- First we show how to construct the Galois field of GF($2^k$)
- In order to construct and the Galois field of $2^k$ elements, we need to represent the elements of GF($2^k$), and we also need to show how we can perform the field operations: addition, subtraction, multiplication, and division (inversion) operations using this representation
- It turns out there are more than one way to do that, for example, polynomial representation and normal representation
- First we will show how to represent field elements using polynomials, and its associated arithmetic

# Representing the Elements of GF($2^k$)

- The polynomial representation of the Galois field of GF($2^k$) is based on the arithmetic of polynomials whose coefficients are from the base field GF(2) and whose degree is at most $k-1$
- The elements of GF($2^k$) is polynomials whose degree is at most $k-1$ and coefficients from GF(2), that is $\{0,1\}$
- Let $a(x), b(x) \in$ GF($2^k$), then they are written as

$$\begin{aligned} a(x) &= a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 \\ b(x) &= b_{k-1}x^{k-1} + \cdots + b_1 x + b_0 \end{aligned}$$

such that $a_i, b_i \in \{0,1\}$

# Addition and Multiplication in GF($2^k$)

- The field addition $c(x) = a(x) + b(x)$ is performed by polynomial addition, where the coefficients are added in GF(2), therefore,

  $$c(x) = a(x) + b(x) = c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$$

  where $c_i = a_i + b_i \pmod 2$
- On the other hand, the field multiplication is performed by first multiplying the polynomials, which would give a polynomial of degree at most $2k - 2$
- Then, we reduce the product polynomial modulo an **irreducible polynomial** of degree $k$

# Construction of GF($2^k$)

- Therefore, in order to construct a Galois field GF($2^k$), we need an irreducible polynomial of degree $k$
- Irreducible polynomials of any degree exist, in fact, usually there are more than one for a given $k$
- We can use any one of these degree $k$ irreducible polynomials, and construct the field GF($2^k$)
- It does not matter which one we choose — we just have to choose one and use that one only
- All such GF($2^k$) fields are isomorphic to one another

# Irreducible Polynomials over GF(2)

| $k$ | irreducible polynomials | | |
|---|---|---|---|
| 1 | $x$ | $x+1$ | |
| 2 | $x^2+x+1$ | | |
| 3 | $x^3+x+1$ | $x^3+x^2+1$ | |
| 4 | $x^4+x+1$ | $x^4+x^3+1$ | $x^4+x^3+x^2+x+1$ |
| 5 | $x^5+x^2+1$ | $x^5+x^3+1$ | $x^5+x^3+x^2+x+1$ |
| | $x^5+x^4+x^3+x+1$ | $x^5+x^4+x^3+x^2+1$ | $x^5+x^4+x^2+x+1$ |
| 6 | $x^6+x+1$ | $x^6+x^3+1$ | $x^6+x^5+1$ |
| | $x^6+x^4+x^2+x+1$ | $x^6+x^4+x^3+x+1$ | $x^6+x^5+x^2+x+1$ |
| | $x^6+x^5+x^3+x^2+1$ | $x^6+x^5+x^4+x^2+1$ | $x^6+x^5+x^4+x+1$ |
| 7 | $x^7+x+1$ | $x^7+x^3+1$ | $x^7+x^4+1$ |
| | $x^7+x^6+1$ | $x^7+x^3+x^2+x+1$ | $x^7+x^5+x^2+x+1$ |
| | $x^7+x^5+x^3+x+1$ | $x^7+x^6+x^3+x+1$ | $x^7+x^4+x^4+x+1$ |
| | $x^7+x^4+x^3+x^2+1$ | $x^7+x^6+x^4+x^2+1$ | $x^7+x^6+x^5+x^2+1$ |
| | $x^7+x^5+x^4+x^3+1$ | $x^7+x^6+x^5+x^4+1$ | |

# Irreducible Polynomials over GF(2)

| $k$ | irreducible polynomials | | |
|---|---|---|---|
| 8 | $x^8+x^4+x^3+x+1$ | $x^8+x^7+x^2+x+1$ | $x^8+x^5+x^3+x+1$ |
| | $x^8+x^7+x^2+x+1$ | $x^8+x^6+x^5+x+1$ | $x^8+x^7+x^5+x+1$ |
| | $x^8+x^7+x^6+x+1$ | $x^8+x^4+x^3+x^2+1$ | $x^8+x^5+x^3+x^2+1$ |
| | $x^8+x^6+x^3+x^2+1$ | $x^8+x^7+x^3+x^2+1$ | $x^8+x^6+x^5+x^2+1$ |
| | $x^8+x^5+x^4+x^3+1$ | $x^8+x^6+x^5+x^3+1$ | $x^8+x^7+x^5+x^3+1$ |
| | $x^8+x^6+x^5+x^4+1$ | $x^8+x^7+x^5+x^4+1$ | |
| 257 | $x^{257}+x^{12}+1$ | $x^{257}+x^{41}+1$ | $x^{257}+x^{48}+1$ |
| | $x^{257}+x^{51}+1$ | $x^{257}+x^{65}+1$ | $x^{257}+x^{192}+1$ |
| | $x^{257}+x^{206}+1$ | $x^{257}+x^{209}+1$ | $x^{257}+x^{216}+1$ |
| | $x^{257}+x^{245}+1$ | | |

# Construction of GF($2^2$)

- GF($2^2$) has $2^2 = 4$ elements: $\{0, 1, x, x+1\}$
- The field addition is performed by adding the field elements, where the coefficients are added in GF(2)

| $+$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x+1$ |
| $1$ | $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x+1$ | $x$ | $1$ | $0$ |

- To perform field multiplication in GF($2^2$), we need an irreducible polynomial of degree 2
- There exists only one irreducible polynomial of degree 2 which is $p(x) = x^2 + x + 1$

# Multiplication in GF($2^2$)

- Multiplication in GF($2^2$) is performed by first multiplying the given input polynomials, where the coefficient arithmetic is performed in GF(2), and reducing the result mod $p(x) = x^2 + x + 1$
- For example, if $a(x) = x$ and $b(x) = x + 1$, then we have

$$c(x) = x \cdot (x + 1) = x^2 + x$$

- We now divide $c(x)$ by $p(x)$ and find the remainder $r(x)$ as

$$\begin{array}{l|l} x^2 + x & \; x^2 + x + 1 \\ \cline{2-2} \underline{x^2 + x + 1} & \; 1 \\ 1 & \end{array}$$

Since $r(x) = 1$, the product of $x$ and $x + 1$ in GF($2^2$) is equal to 1

# Multiplication in GF($2^2$)

- We only need perform reduction mod $p(x)$ if the degree of the resulting polynomial is more than 1
- Reduction mod $p(x)$ brings down the degree to $k$, and therefore, finding an element of GF($2^k$) which are polynomials whose coefficients are in GF(2) and the degree at most $k-1$
- If we continue with the construction of the multiplication table for GF($2^2$), we find the following

| $\times$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x+1$ |
| $x$ | $0$ | $x$ | $x+1$ | $1$ |
| $x+1$ | $0$ | $x+1$ | $1$ | $x$ |

# Representing the Elements of GF($2^k$)

- An element $a(x)$ of GF($2^k$) is a polynomial of degree at most $k-1$, with coefficients from GF(2), as

$$a(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

- While the polynomial representation is the natural representation of the elements of GF($2^k$), we can also represent $a(x)$ using the coefficient vector as $(a_{k-1} \cdots a_1 a_0)$
- This is a binary vector, but it should not be confused with binary numbers
- Whenever we perform arithmetic with these vectors, we need to make sure that they are correctly operated on, for example, addition of $a(x)$ and $b(x)$ using their binary vector representation is performed by adding the individual vector bits mod 2

# Construction of GF($2^3$)

- GF($2^3$) has $2^3 = 8$ elements:

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

- We can represent the field elements more compactly using the binary vectors as $\{000, 001, 010, 011, 100, 101, 110, 111\}$, for example, 011 represents $x+1$, 100 represents $x^2$, and so on
- The field addition is performed by adding coefficients in GF(2), which corresponds to bitwise XOR operation

$$\begin{array}{rr} & 011 \\ \oplus & 110 \\ \hline & 101 \end{array} \qquad \begin{array}{rr} & x+1 \\ + & x^2+x \\ \hline & x^2+1 \end{array}$$

# Addition Table in GF($2^3$)

| + | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| 000 | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 001 | 001 | 000 | 011 | 010 | 101 | 100 | 111 | 110 |
| 010 | 010 | 011 | 000 | 001 | 110 | 111 | 100 | 101 |
| 011 | 011 | 010 | 001 | 000 | 111 | 110 | 101 | 100 |
| 100 | 100 | 101 | 110 | 111 | 000 | 001 | 010 | 011 |
| 101 | 101 | 100 | 111 | 110 | 001 | 000 | 011 | 010 |
| 110 | 110 | 111 | 100 | 101 | 010 | 011 | 000 | 001 |
| 111 | 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |

# Multiplication Table in GF($2^3$)

- To perform multiplication in GF($2^3$), we need a polynomial of degree 3 over GF(2), which we select from the list as $p(x) = x^3 + x + 1$

| $\times$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 |
| 001 | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 010 | 000 | 010 | 100 | 110 | 011 | 001 | 111 | 101 |
| 011 | 000 | 011 | 110 | 101 | 111 | 100 | 001 | 010 |
| 100 | 000 | 100 | 011 | 111 | 110 | 010 | 101 | 001 |
| 101 | 000 | 101 | 001 | 100 | $\boxed{010}$ | 111 | 011 | 110 |
| 110 | 000 | 110 | 111 | 001 | 101 | 011 | 001 | 100 |
| 111 | 000 | 111 | 101 | 010 | 001 | 110 | 100 | 011 |

- An example: $101 \cdot 100 \rightarrow (x^2 + 1) \cdot x^2 = x^4 + x^2$, then the reduction gives the product as $x^4 + x^2 = x \pmod{x^3 + x + 1}$ which is 010

# The Galois Field GF($3^2$)

- We have seen that the elements of GF(3) are $\{0, 1, 2\}$ while its arithmetic is addition and multiplication modulo 3
- Similar to the GF($2^k$) case, in order to construct the Galois field GF($3^k$), we need polynomials degree at most $k-1$ whose coefficients are in GF(3)
- For example, GF($3^2$) has 9 elements and they are of the form $a_1x + a_0$, where $a_1, a_0 \in \{0, 1, 2\}$, which is given as

$$\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

- The addition is performed by polynomial addition, where the coefficient arithmetic is mod 3, for example:

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

# Multiplication in GF($3^2$)

- In order to perform multiplication in GF($3^2$), we need an irreducible polynomial of degree 2 over GF(3)
- This polynomial will be of the form $x^2 + ax + b$ such that $a, b \in \{0, 1, 2\}$
- Note that $b \neq 0$ (otherwise, we would have $x^2 + ax$ which is reducible)
- Therefore, all possible irreducible candidates are

$$x^2 + 1,\ x^2 + 2,\ x^2 + x + 1,\ x^2 + x + 2,\ x^2 + 2x + 1,\ x^2 + 2x + 2$$

- A quick check shows that $x^2 + 1$ is irreducible
- The other two irreducible polynomials are $x^2 + x + 2$ and $x^2 + 2x + 2$

# Multiplication in GF($3^2$)

- Multiplication of $a(x)$ and $b(x)$ in GF($3^2$) can be performed using

$$c(x) = a(x) \cdot b(x) \pmod{x^2+1}$$

- For example, $a(x) = x + 1$ and $b = 2x + 1$ gives

$$\begin{aligned} c(x) &= (x+1)\cdot(2x+1) \pmod{x^2+1} \\ &= 2x^2 + 3x + 1 \pmod{x^2+1} \\ &= 2x^2 + 1 \pmod{x^2+1} \\ &= 2 \end{aligned}$$

- Note in the construction of a Galois field, we select and use only one of the irreducible polynomials

# The Galois Field GF($2^8$)

- The Galois field GF($2^8$) has $2^8 = 256$ elements:

$$\{0, 1, x, x+1, x^2, x^2+1, \ldots, x^7+x^6+x^5+x^4+x^3+x^2+x+1\}$$

- We can represent the field elements using the binary vectors of length 8 (or simply bytes) as $\{00000000, 00000001, \ldots, 11111110, 11111111\}$
- The addition and multiplication tables are quite large, each of which has 256 rows and 256 columns, and each entry is 8 bits (1 byte), requiring $256 \times 256 = 64k$ bytes of memory space for each table
- GF($2^8$) is the building block of the Advanced Encryption Standard
- The irreducible polynomial is $\boxed{p(x) = x^8 + x^4 + x^3 + x + 1}$