Fields in Cryptography

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 $\oplus$ forms an additive group denoted by $G_a = (S, \oplus)$ such that 0 is the neutral element of G_a
- Also the set $S^* = S - \{0\}$ and the multiplication operation $\otimes$ forms a multiplicative group denoted by $G_m = (S^*, \otimes)$ such that 1 is the unit (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 equal to zero, if the repeated sum never reaches the additive identity element 0

Rings

- The set of integers $\mathcal{Z}$ with the integer addition and multiplication operation does not form a field
- We can easily verify that $(\mathcal{Z}, +)$ is an additive group with identity 0
- However, $(\mathcal{Z} - \{0\}, \cdot)$ 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 $2 \cdot x = 1$
- In fact, $(\mathcal{Z}, +, \cdot)$ forms a **ring**
- Ring is 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 addition and multiplication operations forms a field, such that the additive and multiplicative identities are 0 and 1
- Indeed, $(\mathcal{Q}, +)$ is an additive group with identity 0
- The additive inverse of $\frac{a}{b}$ is found as $-\frac{a}{b}$
- Also, $(\mathcal{Q}, \cdot)$ 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 be equal to 0 if we take zero 1

Infinite Fields

- Similarly, the set of real numbers $\mathcal{R}$ together with the addition and multiplication operations forms a field, such that the additive and multiplicative identities are 0 and 1
- Also, the set of complex numbers $\mathcal{C}$ together with the addition and multiplication operations forms a field, such that the additive and multiplicative identities are 0 and 1
- 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
- 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
- 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

- 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 denote this field by GF(p) or $\mathcal{F}_p$
- It is called a field of p elements or 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 $(\mathcal{Z}_p^*, \cdot)$ 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

$$\overbrace{1 + 1 + 1 + \cdots + 1}^{p \text{ copies of } 1} = 0$$

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 field size is 2, and the field 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

$\cdot$	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 field size is 3, and the field characteristic is 3
- The additive identity is 0 while the multiplicative identity is 1
  the additive group: $(\{0, 1, 2\}, +)$, the multiplicative group: $(\{1, 2\}, \cdot)$
- 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

·	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

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

- However, there may be another way to construct a field of 6 elements

Finite Fields of Size Prime Power

- It turns out there is no way to construct a field of 6 elements
- Galois showed that the size of a finite field can either be prime or power of a prime: 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 the set $\mathcal{Z}_p$
- How does one construct GF(p^2) or GF(p^3)?
- 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 $a(\alpha), b(\alpha) \in$ GF(2^k), then they are written as polynomials

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

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

Addition and Multiplication in GF(2^k)

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

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

  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	α	$\alpha+1$	
2	$\alpha^2+\alpha+1$		
3	$\alpha^3+\alpha+1$	$\alpha^3+\alpha^2+1$	
4	$\alpha^4+\alpha+1$	$\alpha^4+\alpha^3+1$	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$
5	$\alpha^5+\alpha^2+1$	$\alpha^5+\alpha^3+1$	$\alpha^5+\alpha^3+\alpha^2+\alpha+1$
	$\alpha^5+\alpha^4+\alpha^3+\alpha+1$	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	$\alpha^5+\alpha^4+\alpha^2+\alpha+1$
6	$\alpha^6+\alpha+1$	$\alpha^6+\alpha^3+1$	$\alpha^6+\alpha^5+1$
	$\alpha^6+\alpha^4+\alpha^2+\alpha+1$	$\alpha^6+\alpha^4+\alpha^3+\alpha+1$	$\alpha^6+\alpha^5+\alpha^2+\alpha+1$
	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	$\alpha^6+\alpha^5+\alpha^4+\alpha+1$
7	$\alpha^7+\alpha+1$	$\alpha^7+\alpha^3+1$	$\alpha^7+\alpha^4+1$
	$\alpha^7+\alpha^6+1$	$\alpha^7+\alpha^3+\alpha^2+\alpha+1$	$\alpha^7+\alpha^5+\alpha^2+\alpha+1$
	$\alpha^7+\alpha^5+\alpha^3+\alpha+1$	$\alpha^7+\alpha^6+\alpha^3+\alpha+1$	$\alpha^7+\alpha^4+\alpha^4+\alpha+1$
	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+1$	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+1$	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+1$
	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+1$	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+1$	

Irreducible Polynomials over GF(2)

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

Construction of GF(2^2)

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

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	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 $p(\alpha) = \alpha^2 + \alpha + 1$

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 $p(\alpha) = \alpha^2 + \alpha + 1$
- For example, if $a(\alpha) = \alpha$ and $b(\alpha) = \alpha + 1$, then we have

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

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

$$\begin{array}{l|l} \alpha^2 + \alpha & \alpha^2 + \alpha + 1 \\ \cline{2-2} \alpha^2 + \alpha + 1 & 1 \\ \hline 1 & \end{array}$$

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

Multiplication in GF(2^2)

- We only need perform reduction mod $p(\alpha)$ if the degree of the resulting polynomial is more than 1
- Reduction mod $p(\alpha)$ 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

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Representing the Elements of GF(2^k)

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

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

- While the polynomial representation is the natural representation of the elements of GF(2^k), we can also represent $a(\alpha)$ 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 representation of integers
- Whenever we perform arithmetic with these vectors, we need to make sure that they are correctly operated on, for example, addition of $a(\alpha)$ and $b(\alpha)$ 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:

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

- 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 $\alpha+1$, 100 represents α^2, and so on
- The field addition is performed by adding coefficients in GF(2), which corresponds to bitwise XOR operation

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

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 $p(\alpha) = \alpha^3 + \alpha + 1$

$\cdot$	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	010	111	011	110
110	000	110	111	001	101	011	001	100
111	000	111	101	010	001	110	100	011

- An example: $101 \cdot 100 \rightarrow (\alpha^2 + 1) \cdot \alpha^2 = \alpha^4 + \alpha^2$, then the reduction gives the product as $\alpha^4 + \alpha^2 = \alpha \pmod{\alpha^3 + \alpha + 1}$ 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 $a_1\alpha + a_0$, where $a_1, a_0 \in \{0, 1, 2\}$, which is given as

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

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

$$(\alpha + 1) + (\alpha + 2) = 2\alpha$$

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 $\alpha^2 + a\alpha + b$ such that $a, b \in \{0, 1, 2\}$
- Note that $b \neq 0$ (otherwise, we would have $\alpha^2 + a\alpha$ which is reducible)
- Therefore, all possible irreducible candidates are

$$\alpha^2 + 1,\ \alpha^2 + 2,\ \alpha^2 + \alpha + 1,\ \alpha^2 + \alpha + 2,\ \alpha^2 + 2\alpha + 1,\ \alpha^2 + 2\alpha + 2$$

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

Multiplication in GF(3^2)

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

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

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

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

- 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:

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

- We represent the field elements using the binary vectors of length 8 $\{00000000, 00000001, \ldots, 11111110, 11111111\}$
- 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 $256 \cdot 256 = 64k$ bytes of memory space for each table
- $GF(2^8)$ is the building block of the Advanced Encryption Standard
- AES uses the irreducible polynomial $\boxed{p(\alpha) = \alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1}$

Inversion in $\mathrm{GF}(2^k)$

- Given $a \in \mathrm{GF}(2^k)$, its multiplicative inverse $a^{-1} \in \mathrm{GF}(2^k)$ is also in the field, and is the element with the property $a \cdot a^{-1} = 1$, except when $a = 0$
- The additive inverse $-a$ in fields of characteristic 2 is the element itself: $a + a = 0$
- There are various ways to compute the multiplicative inverse, for example, the extended Euclidean algorithm or Fermat's theorem
- Since the multiplicative group of $\mathrm{GF}(2^k)$ is of order $2^k - 1$, for any nonzero $a \in \mathrm{GF}(2^k)$, we have $a^{2^k-1} = 1$
- Therefore, a^{-1} can be computed using $a^{-1} = a^{2^k-2}$ since

$$a \cdot a^{2^k-2} = a^{2^k-1} = 1$$