Scribe: Cryptography and Network Security (Class.22.B)

Shubham Mishra

12-Oct-2020

1 Finite Fields

A field $(R, +, \cdot)$ is called a finite field if R is a finite set.

The number of elements in a finite field is called the **order** of the field. For example, the field $\mathbb{F}_2$ with elements $\{0, 1\}$ along with exclusive OR and AND operations form a finite field with order, $o = 2$.

The minimum λ for which $1 + 1 + ...\lambda times = 0$ is called the **characteristic** of the field.[2]

Finite fields are also called **Galois Fields**[1].

Theorem: The characteristic of a finite field is always a prime.

Proof: If possible, let the characteristic λ be a composite number $\lambda = pq$, where $p, q > 1$.

Then $1+1+1+...\lambda times = p1+p1+...qtimes = p1 \cdot q1 = 0$, since multiplication distributes over addition and $1 \cdot 1 = 1$.

Now, a field does not have a zero divisor. Hence either $p = 0$ or $q = 0$, which is contradiction.

Hence the characteristic must be a prime.

Note: The definition of characteristic can be extended to λ times addition of any element a of the field.

Theorem: The order of a finite field is given by p^m for the characteristic prime p and some integer m.

Proof: Consider a subfield of the given field with p elements. We can define a vector space over this field with vectors of the form $(a_1, a_2, ..., a_m) \forall a_i \in$ the subfield. Clearly, we can have a bijection from the vector space to our original field.

There are total p^m elements in the Vector Space. Hence the total number of elements in the field must also be p^m.

1.1 Galois Field 2^n

Generally we represent a Galois field $GF(p) = \{0, 1, ..., p-1\}$ where p is prime number.

But the representation of $GF(p^m)$ is different.

We take the simplest case when $p = 2$. So, $GF(2) = \{0, 1\}$. But $GF(2^n)$ is represented by a polynomial of degree $(n-1)$, for example,

$b(x) = b_{n-1}x^{n-1} + b_{n-1}x^{n-2} + ... + b_0$

is a member of $GF(2^n)$ for some $b_i \in \{0, 1\}$.

The set of polynomials over a field F with degree less than l is denoted by $F[x]|_l$. Here F is called the **base field**.

In memory, $GF(2^n)$ is represented as a bit-string of length n, whose LSB represents the constant term and the MSB the highest power term's coefficient.

For example, the polynomial $x^5 + x^3 + x^2 + 1$ in $GF(2^8)$ as

0	0	1	0	1	1	0	1

.

or in hexadecimal as `2d`.

AES uses $GF(2^8)$.

1.2 Addition in $GF(2^n)$

For 3 polynomials A, B, C in $GF(2^n)$, we define,

$C(x) = A(x) + B(x) \iff c_i = a_i + b_i$

Here c_i, a_i, b_i are the coefficients $\in GF(2)$ of A, B, C respectively.

Note that in $GF(2)$, addition is actually the exclusive OR operation. Since $a \oplus (a \oplus b) = b$, addition is self-inverse in $GF(2)$.

Example: Compute the sum of `57` and `83` in $GF(2^8)$.

Solution: `0x57` = `0b01010111` and `0x83` = `0b10000011`. Hence the corresponding polynomials are $(x^6 + x^4 + x^2 + x + 1)$ and $(x^7 + x + 1)$ respectively.

Now we can do a term by term addition, or we can use the fact that `0x57 ^ 0x83 = 0b11010100` and hence the addition result is $(x^7 + x^6 + x^4 + x^2)$.

1.3 Irreducible Polynomials

A polynomial $d(x)$ is irreducible over the field $GF(p)$ if and only if there exists no two non-unity polynomials $a(x)$ and $b(x)$ with coefficients in $GF(p)$ such that, $d(x) = a(x) \cdot b(x)$.

We can intuitively consider the irreducible polynomials as primes in $GF(2^n)$.

For a fixed n, the irreducible polynomial is not unique. Here we give the possible irreducible polynomials for some degrees.

Degree	Irreducible Polynomial
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1
4	$x^4+x^3+x^2+x+1$, x^4+x^3+1, x^4+x+1

Example: Prove that $(x+1)|(x^4+1)$ and hence x^4+1 is not irreducible.

Solution: We see that, $x+1=0 \implies x=1$.

Let $f(x) = x^4+1$. Now, $f(1) = 1^4+1 = 1+1 = 0$

So x^4+1 and $x+1$ both vanish for same x value. Hence $(x+1)|(x^4+1)$.

Alternative Solution: Notice that $(x^4+1) = (x+1)\cdot(x^3+x^2+x+1)$, which clearly proves the result.

All calculations above were done in $GF(2)$ base field.

1.4 Multiplication in $GF(2^n)$

Multiplication in a field must be: - Closed - Associative - Commutative - Distributive over addition - Multiplicative identity and inverse must exist for all elements.

Usual polynomial multiplication cannot provide closure as multiplication of 2 n degree polynomial results in a polynomial with degree $2n$.

Hence we reduce the polynomial obtained by usual multiplication by an irreducible polynomial.

$C(x) = A(x) \cdot B(x)(mod m(x))$

The irreducible polynomial used should be specified along with the definition of the field. The polynomial used in AES is $x^8+x^4+x^3+x+1$.

Example: Compute the product of `57` and `83` in $GF(2^8)$. Reduce it modulo $(x^8+x^4+x^3+x+1)$.

Solution: The polynomials are $(x^6+x^4+x^2+x+1)$ and (x^7+x+1).

$(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1)$

$= (x^{13} + x^{11} + x^9 + x^8 + x^7) \oplus (x^7 + x^5 + x^3 + x^2 + x) \oplus (x^6 + x^4 + x^2 + x + 1)$

$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$

Now we will factor out our reducing polynomial from the above expression.

$x^8 + x^4 + x^3 + x + 1 = 0$

$\implies x^8 = x^4 + x^3 + x + 1$

$\implies x^9 = x^5 + x^4 + x^2 + x$

$\implies x^{11} = x^7 + x^6 + x^4 + x^3$

$\implies x^{13} = x^9 + x^8 + x^6 + x^5 = (x^5 + x^4 + x + 1) + (x^4 + x^3 + x + 1) + x^6 + x^5 = x^6 + x^3 + x^2 + 1$

Now, $x^{13} + x^{11} + x^9 + x^8 + x^5 + x^4 + x^3 + 1$

$= (x^6 + x^3 + x^2 + 1) + (x^7 + x^6 + x^4 + x^3) + (x^5 + x^4 + x^2 + x) + (x^4 + x^3 + x + 1) + x^6 + x^5 + x^4 + x^3 + 1$

$= x^7 + x^6 + 1$

This is the required product.

2 Introduction to AES

AES stands for **Advanced Encryption Standard**. It is a successor of the Data Encryption Standard (DES) algorithm.

2.1 History of AES[3]

The AES algorithm was chosen using by National Institute of Standards and Technology (NIST) through a series of selection rounds that lasted from 1997 to 2000.

In round 1, 15 algorithms were suggested. Few of them are `CAST-256`, `DFC`, `Rijndael`, `SAFER+` etc. They were judged on their security and performance in low resource environments.

Out of the 15, 5 were selected for the 2nd round: `MARS`, `RC6`, `Rijndael`, `Serpent` and `Twofish`. These are known as *AES finalists*.

NIST organised the AES2 conference, where people voted for these 5 algorithms. A further round of intense cryptanalysis followed and on October 2, 2000, NIST announced Rijndael as the selected algorithm.

The name *"Rijndael"* is a portmanteau of the names of its developers: Vincent Rijmen and Joan Daemon.

2.2 AES Specifications

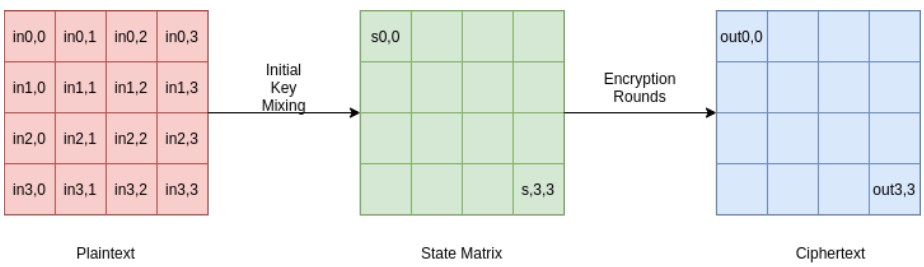
The current standard is actually a subset of the actual Rijndael algorithm. The later works with variable key and block sizes in multiples of 32. AES has fixed the block size to 128 bits. There are 3 key sizes: 128, 192 and 256 bits.

Variant	Key length	Block length	Number of Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

2.3 Overview of AES

AES splits the 128 bit input into a 4x4 matrix where each cell contains 1 byte of data.

The overview of the steps are shown as follows:



Rijndael uses 4 different round functions:

1. Byte Sub
2. Shift Row
3. Mix Column
4. Add Round Key

3 Conclusion

In today's lecture, we learnt about Finite Fields which are very important for understanding the operations in AES.

We also understood the rigorous procedure required to standardise a cryptographic algorithm.

References

[1] Christoforus Juan Benvenuto. Galois field in cryptography, 2012. URL https://sites.math.washington.edu/~morrow/336_12/papers/juan.pdf. [Online; accessed 12-October-2020].

[2] Rajat Mittal. Lecture 8: Finite fields, 2015. URL https://www.cse.iitk.ac.in/users/rmittal/prev_course/s15/notes/ffields.pdf. [Online; accessed 12-October-2020].

[3] Wikipedia contributors. Advanced encryption standard process — Wikipedia, the free encyclopedia, 2020. URL https://en.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard_process&oldid=974916566. [Online; accessed 12-October-2020].