[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Dipean Dasgupta (202151188)

Winter 2023-2024
Lecture (Week 4)

1 Mathematical Recall:

1.1 Binary Operation:

A binary operation on a set is referred as mapping from the same set to the same set. It is denoted by $*$. That is:

$$*=S \times S \quad S=\text{a set}$$

It plays a role that assigns to each ordered pair of elements from S to an element of S.
Properties:
$*(a,b)=c \qquad a,b,c \in S$
$*(b,a)=d \qquad d \in S$
It is not necessary that d=c.

1.2 Group:

A group $(G,*)$ consists of a set G with a binary operation $*$ on G that satisfies the following three conditions:

- The group operation is associative. That is, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in G$.
- There is an element $1 \in G$, called the identity element, such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$.
- For each $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

A group G is abelian (or commutative) if, $a \cdot b = b \cdot a$ for all $a,b \in G$.
A group G is finite if $|G|$ is finite. The number of elements in a finite group is called its order.

Examples of Group:

- (G,*) here G is invertible nxn matrix and $*$ is ordinary matrix multiplication $\rightarrow$ a group
- $(\mathbb{Z},+)$ is a group
- $(\mathbb{Z}$,x) x=multiplication is not a group
- $(Q,*)$ here Q is set of all rational numbers and $*$ is standard multiplication operation $\rightarrow$ a group.
- $(\mathbb{Z}_n,+_n)$ where $\mathbb{Z}_n$ refers to, let's say, $\mathbb{Z}_{26}$ – a group.
- $(\mathbb{Z}_n,*_n)$ where $*_n$ represents multiplication mod n. This is not a group.

- After addition modulo n, the set $_n$ forms a group of order n. Since not every element in the set $_n$ has a multiplicative inverse, the set $_n$ with a multiplication operation modulo n is not a group. On the other hand, the set with identity element 1 is a group of order $o(n)$ under multiplication modulo n.

- If H is a group in and of itself with regard to the operation of G, then a non-empty subset H of a group G is a subgroup of G. A proper subgroup of G is defined as H if it is a subgroup of G and $H \subset G$.

- If there is an element $a \in G$ such that for every $b \in G$, there exists an integer i such that $b = a^i$, then G is cyclic. We refer to such an element a as a generator of G.

- The set of all powers of a forms a cyclic subgroup of G, known as the subgroup formed by a and denoted by (a), if G is a group and $a \in G$.

- Let $a \in G$ and G be a group. If such an integer exists, the order of a is defined as the least positive integer t such that $a = 1$. The order of a is defined as ∞ if such a t does not exist.

- Let $a \in G$ be an element of finite order t, and let G be a group. The subgroup produced by a has a size of $|(a)|$, which equals t.

- (Lagrange's theorem) $|H|$ divides $|G|$ if G is a finite group and H is a subgroup of G. Therefore, the order of a divides $|G|$ if $a \in G$.

- A cyclic group G has cyclic subgroups; all of them are cyclic. In fact, if G is a cyclic group of order n, then G has exactly one subgroup of order d for each positive divisor d of n.

- Let G be a group.
  - If the order of $a \in G$ is t, then the order of a^k is $t \ / \ \gcd(t, k)$.
  - If G is a cyclic group of order n and d divides n, then G has exactly $\phi(d)$ elements of order d. In particular, G has $\phi(n)$ generators.

1.3 Ring:

A ring $(R, +, \times)$ consists of a set R with two binary operations arbitrarily denoted $+$ (addition) and $\times$ (multiplication) on R, satisfying the following axioms:

- $(R, +)$ is an abelian group with identity denoted 0.

- The operation $\times$ is associative. That is, $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.

- There is a multiplicative identity denoted 1, with $1 = 0$, such that $1 \times a = a \times 1 = a$ for all $a \in R$.

- The operation $\times$ is distributive over $+$. That is, $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$ for all $a, b, c \in R$.

The ring is commutative if $a \times b = b \times a$ for all $a, b \in R$.

- The set of integers with the usual operations of addition and multiplication is a commutative ring.

- The set $_n$ with addition and multiplication performed modulo n is a commutative ring.

- An element a of a ring R is called a unit or an invertible element if there is an element $b \in R$ such that $a \times b = 1$.
- The set of units in a ring R forms a group under multiplication, called the group of units of R.
- The group of units of the ring $\mathbb{Z}_n$ is $\mathbb{Z}_n^*$.

1.4 Fields:

A field is a non-empty set F together with 2 binary operations +(addition) and *(multiplication) where the following properties are satisfied:

- (F,+) is a abelian group
- If Q_F denotes the additive identity element of (F,t) then $(F \setminus \{O_F\}, *)$ is a commutative or abelian group.
- $\forall a, b, c \in Fwehavea * (b + c) = (a * b) + (a * c)$
- $(z, +, .) \rightarrow NotField \quad (Q, +, .) \rightarrow isafield$. Here, Z is set of integers and Q is set of rational numbers.
  0 is additive identity and 1 is multiplicative identity.
  $(Q \setminus \{0\}, .)$ is a commutative group.
- $F_p = 0, 1, 2 \ldots p - 1$ p=prime number.
  so, $(F_p, +_p, *_p) :\rightarrow Field$
  - $+_p : (x + y)(modp) \rightarrow commutative$
  - $*_p : (x.y)(modp) \rightarrow commutative$
- A field is a commutative ring with multiplicative inverses for each non-zero element.
- The *characteristic* of a field $\mathbb{F}$ is 0 if $1+1+\cdots+1$ is never equal to 0 for any $m \geq 1$. Otherwise, the characteristic of the field is the least positive integer m such that $\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = 0$.
- Since 1 and -1 are the only non-zero integers with multiplicative inverses, the set of integers $mathbbZ$ under the standard addition and multiplication operations is not a field. Nonetheless, under standard operations, the rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ form fields of characteristic 0.
- If and only if n is a prime number, then $\mathbb{Z}_n$ is a field (under the standard addition and multiplication operations modulo n). $\mathbb{Z}_n$ has characteristic n if n is prime.
- A field's characteristic m is a prime number if it is not 0.
- If $\mathbb{F}$ is a field in and of itself with respect to the operations of $\mathbb{E}$, then a subset $\mathbb{F}$ of a field $\mathbb{E}$ is an *subfield* of $\mathbb{E}$. $\mathbb{E}$ is considered an *extension field* of if this is the case.

1.4.1 Field Extension:

Suppose k_2 is a field with addition(+) and multiplication(∗). Let $k_1 \subset$k$_2$ be closed under both operations such that k_1 itself is a field for the restrictions of + and ∗ to the set k_1; then k_1 is called a *subfield* of k_2 and k_2 is therefore a *Field Extension* of k_1.
$F \to Field\ (F, +, .)$
$F[x] = a_0 + a_1x + a_2x^2 \ldots | a_i \in F$ Here x is Polynomial Ring.
$F[x] = a_0 + a_1x + a_2x^2 \ldots a_{n-1}x^{n-1} | a_i \in F$
Addition of Field:

$$(a_0 + a_1x + \ldots a_{n-1}x^{n-1}) + (b_0 + b_1x + \ldots b_{n-1}x^{n-1}) \\ = (\mathrm{a}_0 + b_0) + (a_1 + b_1)x + \ldots x^n$$

so, $a_i + b_i =$ additive operation of a field.
Multiplication of Field:

$$(a_0 + a_1x + \ldots a_{n-1}x^{n-1}) * (b_0 + b_1x + \ldots b_{n-1}x^{n-1}) \\ = (\mathrm{a}_0 * b_0) + (a_0 * b_1 + a_1 * b_0)x + \ldots (a_n * b_{n-1})x^{2n-2}$$

(F[x],+,*) is a ring.

1.5 Polynomial Rings:

If R is a commutative ring, then a polynomial in the indeterminate x over the ring R is an expression of the form

$$f(x) = a_nx^n + \cdots + a_2x^2 + a_1x + a_0,$$

where each $a_i \in R$ and $n \geq 0$.
The coefficient of x^i in $f(x)$ is denoted by the element a_i. The degree of $f(x)$, or deg $f(x)$, is the greatest integer m for which $a_m \neq 0$; a_m is known as the leading coefficient of $f(x)$. $f(x)$ has degree 0 if $f(x) = a_0$ (a constant polynomial) and $a_0 \neq 0$.
$f(x)$ is referred to as the zero polynomial if all of its coefficients are 0. For mathematical convenience, its degree is specified as $-\infty$.
If the leading coefficient of the polynomial $f(x)$ is equal to 1, it is referred to as monic.
The polynomial ring $R[x]$ is the ring formed by the set of all polynomials in the indeterminate x with coefficients from R, if R is a commutative ring. The two operations are addition and multiplication of standard polynomials, with coefficient arithmetic carried out in the ring R.

A polynomial $P(x) \in F[x]$ of degree n is called irreducible if it cannot be written as $P_1(x) * P_2(x)$ with $P_1(x), P_2(x) \in F[x]$ and the degree of both $P_1(x)$ and $P_2(x)$ being 1.

The set $I = \langle P(x) \rangle = f(x) \cdot P(x) | f(x) \in F[x]$ is an ideal in $F[x]$. It is the set of all multiples of $P(x)$.
The division set modulo $P(x)$ is defined as:

[F[x] / $\langle < P(x) \rangle >= \langle q(x) + \langle < P(x) \rangle > | q(x) \in F[x] \rangle]$
Where $q(a) \in F[x]$ and $q(x) = r(x) + \langle P(2) \rangle$ with $r(x) \in F[x] / \langle P(2) \rangle$.
($[F[x] / \langle P(x) \rangle$,+,*)

2 Advanced Encryption Standard(AES):

One popular symmetric key encryption technique for protecting data is AES (Advanced Encryption Standard). It superseded the previous Data Encryption Standard (DES) when it was made a federal standard in 2001 by the National Institute of Standards and Technology (NIST). With support for key sizes of **128, 192, or 256 bits**, AES functions on data blocks.
Whereas DES employs a Feistel structure, AES functions more like a substitution-permutation network. The state, a 4-by-4 array of bytes, is changed repeatedly in rounds during the AES algorithm's execution. The cipher's input, which is 128 bits, or precisely 16 bytes, is what the state is originally set to. Next, in four phases every round, the state is subjected to the following operations:

- **S1: Add RoundKey**: The master key is used to generate a 128-bit sub-key, which is represented as a 4-by-4 array of bytes, for each AES round. This sub-key is used to XOR the state array, updating it.
- **S2: SubBytes:** In this stage, a single fixed lookup table S is used to replace each byte in the state array with a new byte. The S-box, often known as the substitution table, is a bijection over $\{0,1\}^8$
- **S3: ShiftRows:** During this phase, the bytes in every row of the state array are moved to the left in the following order: the array's first row remains unaltered, while the second, third, and fourth rows are moved one, two, and three places to the left, respectively. Every shift is cyclical, thus the first byte in the second row, for example, becomes the fourth byte.
- **S4: MixColumns**: The four bytes in each column undergo an invertible transformation in this stage. (In technical terms, this is a matrix multiplication over an appropriate field, or a linear transformation.) This transformation's feature is that it produces two outputs that differ by at least 5 — b bytes if two inputs differ by b ¿ 0 bytes when applied.

AddRoundKey takes the place of MixColumns in the last round. This keeps an enemy from just flipping the final three steps, which are independent of the key. For this reason, despite being more difficult to develop, AES is now commonly utilized because it is far stronger than DES and triple DES.

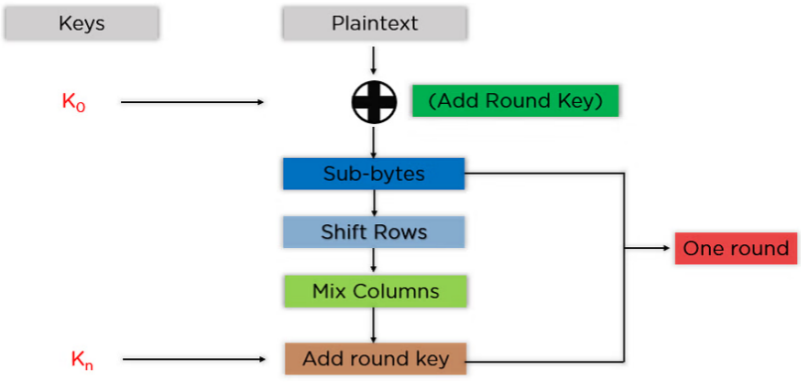

Figure:AES Encryption
Source:Simplilearn

2.1 Working Principles:

Instead of working with bits, AES works with bytes of data. The cipher processes 128 bits, or 16 bytes, of the incoming data at a moment because the block size is 128 bits. The key length determines how many rounds there are:

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

2.1.1 Creating Round Keys:

To determine every round key from the key, an algorithm known as the Key Schedule is employed. In order to generate a variety of round keys for the associated encryption round, the beginning key is used.
A sequence of round keys with the same length as the AES block size are produced by this technique. Round keys are produced by combining circular shifting of bytes, substitution via the S-box, and XOR operations. Every round of the encryption procedure uses these round keys, which increase security by causing confusion and dispersion. For particular operations, the last round of encryption uses the final round key.

2.1.2 ENCRYPTION:

Every block is viewed by AES as a 16-byte (4-byte x 4-byte = 128-byte) grid arranged in columns.

b0	b4	b8	b12
b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15

Each round comprises of 4 steps:

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The MixColumns round is absent from the previous round. The algorithm's SubBytes handle substitution, while MixColumns and ShiftRows handle permutation.

SubBytes:
The substitution is put into practice in this stage. Every byte is changed to a different byte in

this stage. The S-box, also known as a lookup table, is used to carry it out. The manner this replacement is carried out ensures that a byte is never replaced by itself or by a byte that is a compliment of the one that is being replaced.
As before, this step yields a 16 byte (4 x 4) matrix. The permutation is implemented in the next two phases.

ShiftRows:
This action is exactly what it sounds like. We move each row a certain amount of times. There is no shift to the top row. There is one leftward movement of the second row. There are two leftward shifts to the third row. There are three leftward shifts to the fourth row. (A circular shift to the left is executed.)

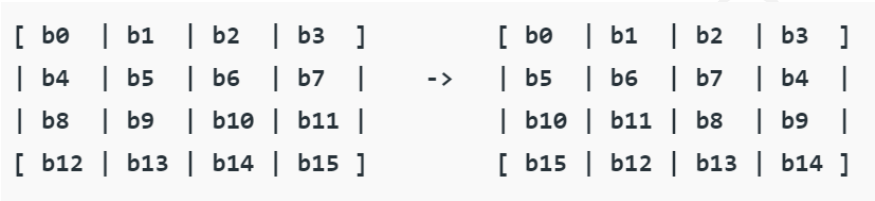

Figure: Shifting of Rows
Source:GeeksForGeeks

MixColumns:
Essentially, matrix multiplication is what this step entails. Every column is multiplied by a particular matrix, which modifies each byte's location within the column. In the previous round, this step is omitted.
The relevant round key is now XORed with the output of the preceding step. In this case, the 16 bytes are simply regarded as 128 bits of data rather than a grid.

Following each of these rounds, 128 bits of encrypted data are returned as the output. Until all of the data that has to be encrypted has gone through this process, it is repeated.