

Introduction to Modern Cryptography

Lecture 3

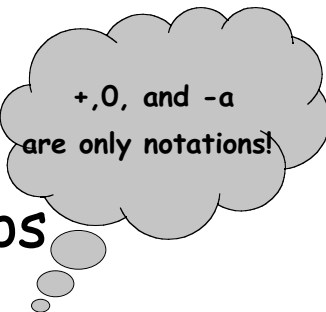
(1) Finite Groups, Rings and Fields

(2) AES - Advanced Encryption Standard

Sub-groups

- Let $(G, +)$ be a group, $(H, +)$ is a sub-group of $(G, +)$ if it is a group, and $H \subseteq G$.
- Claim: Let $(G, +)$ be a finite group, and $H \subseteq G$. If H is closed under $+$, then $(H, +)$ is a sub-group of $(G, +)$.
- Examples
- Lagrange theorem: if G is finite and $(H, +)$ is a sub-group of $(G, +)$ then $|H|$ divides $|G|$

Review - Groups



$+$, 0 , and $-a$
are only notations!

Def (group): A set G with a binary operation $+$ (addition) is called a commutative *group* if

$$1 \quad \forall a, b \in G, a+b \in G$$

$$2 \quad \forall a, b, c \in G, (a+b)+c = a+(b+c)$$

$$3 \quad \forall a, b \in G, a+b = b+a$$

$$4 \quad \exists 0 \in G, \forall a \in G, a+0 = a$$

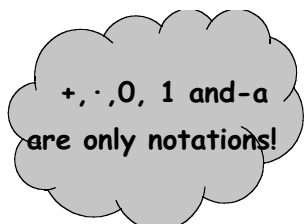
$$5 \quad \forall a \in G, \exists -a \in G, a+(-a) = 0$$

Order of Elements

- Let a^n denote $a + \dots + a$ (n times)
- We say that a is of order n if $a^n = 0$, and for any $m < n$, $a^m \neq 0$
- Examples
- Euler theorem: In the multiplicative group of Z_m , every element is of order at most $\phi(m)$.

Cyclic Groups

- Claim: let G be a group and a be an element of order n . The set $\langle a \rangle = \{1, a, \dots, a^{n-1}\}$ is a sub-group of G .
- a is called the *generator* of $\langle a \rangle$.
- If G is generated by a , then G is called *cyclic*, and a is called a *primitive element* of G .
- Theorem: for any prime p , the multiplicative group of Z_p is cyclic



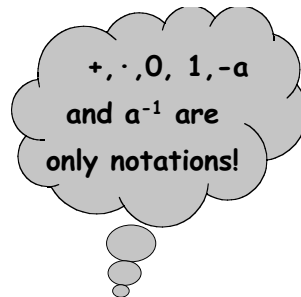
Review - Rings

Def (ring): A set F with two binary operations $+$ (addition) and \cdot (multiplication) is called a commutative *ring* with identity if

- | | |
|---|--|
| 1 $\forall a, b \in F, a+b \in F$ | 6 $\forall a, b \in F, a \cdot b \in F$ |
| 2 $\forall a, b, c \in F, (a+b)+c = a+(b+c)$ | 7 $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ |
| 3 $\forall a, b \in F, a+b = b+a$ | 8 $\forall a, b \in F, a \cdot b = b \cdot a$ |
| 4 $\exists 0 \in F, \forall a \in F, a+0 = a$ | 9 $\exists 1 \in F, \forall a \in F, a \cdot 1 = a$ |
| 5 $\forall a \in F, \exists -a \in F, a+(-a) = 0$ | 10 $\forall a, b, c \in F, a \cdot (b+c) = a \cdot b + a \cdot c$ |

Review - Fields

Def (field): A set F with two binary operations $+$ (addition) and \cdot (multiplication) is called a *field* if



- | | |
|---|--|
| 1 $\forall a, b \in F, a+b \in F$ | 6 $\forall a, b \in F, a \cdot b \in F$ |
| 2 $\forall a, b, c \in F, (a+b)+c = a+(b+c)$ | 7 $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ |
| 3 $\forall a, b \in F, a+b = b+a$ | 8 $\forall a, b \in F, a \cdot b = b \cdot a$ |
| 4 $\exists 0 \in F, \forall a \in F, a+0 = a$ | 9 $\exists 1 \in F, \forall a \in F, a \cdot 1 = a$ |
| 5 $\forall a \in F, \exists -a \in F, a+(-a) = 0$ | 10 $\forall a, b, c \in F, a \cdot (b+c) = a \cdot b + a \cdot c$ |
| 11 $\forall a \neq 0 \in F, \exists a^{-1} \in F, a \cdot a^{-1} = 1$ | |

Review - Fields

A field is a commutative ring with identity where each non-zero element has a multiplicative inverse

$$\forall a \neq 0 \in F, \exists a^{-1} \in F, a \cdot a^{-1} = 1$$

Equivalently, $(F, +)$ is a commutative (additive) group, and $(F \setminus \{0\}, \cdot)$ is a commutative (multiplicative) group.

Polynomials over Fields

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1 \cdot x + a_0$
 be a polynomial of degree n in one variable x over a field
 F (namely $a_n, a_{n-1}, \dots, a_1, a_0 \in F$).

Theorem: The equation $f(x)=0$ has at most n solutions in F .

Remark: The theorem does not hold over rings with identity.
 For example, in Z_{24} the equation $6 \cdot x = 0$
 has six solutions $(0,4,8,12,16,20)$.

Finite Fields

Def (finite field): A field $(F, +, \cdot)$ is called a finite field
 if the set F is finite.

Example: Z_p denotes $\{0,1,\dots,p-1\}$. We define $+$ and \cdot as
 addition and multiplication modulo p , respectively.

One can prove that $(Z_p, +, \cdot)$ is a field iff p is prime.

Q.: Are there any finite fields except $(Z_p, +, \cdot)$?

Polynomial Remainders

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1 \cdot x + a_0$
 $g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \dots + b_1 \cdot x + b_0$
 be two polynomials over F such that $m < n$ (or $m=n$).

Theorem: There is a unique polynomial $r(x)$ of degree $< m$
 over F such that

$$f(x) = h(x) \cdot g(x) + r(x).$$

Remark: $r(x)$ is called the remainder of $f(x)$ modulo $g(x)$.

$$\begin{aligned} > \text{rem}(4 \cdot x^5 + 3 \cdot x^2 + 1, x^3 + 2, x); \\ & \quad 1 - 5x^2 \\ > \text{gcd}(4 \cdot x^5 + 3 \cdot x^2 + 1, x^3 + 2); \\ & \quad 1 \end{aligned}$$

The Characteristic of Finite Fields

Let $(F, +, \cdot)$ be a finite field.

There is a positive integer n such that

$$\underbrace{1 + \dots + 1}_{(n \text{ times})} = 0$$

The minimal such n is called the characteristic of F ,
 $\text{char}(F)$.

Thm: For any finite field F , $\text{char}(F)$ is a prime number.

Galois Fields $GF(p^k)$

Theorem: For every prime power p^k ($k=1,2,\dots$) there is a unique finite field containing p^k elements. These fields are denoted by $GF(p^k)$.

There are no finite fields with other cardinalities.



Évariste Galois (1811-1832)

Remarks:

1. For $F=GF(p^k)$, $\text{char}(F)=p$.
2. $GF(p^k)$ and \mathbb{Z}_{p^k} are not the same!

Irreducible Polynomials

A polynomial is irreducible in $GF(p)$ if it does not factor over $GF(p)$. Otherwise it is reducible.

Examples:

```
Factor(x^5+x^4+x^3+x+1) mod 5;  
      (x+2)(x^3+3x+2)(x+4)  
Factor(x^5+x^4+x^3+x+1) mod 2;  
      x^5+x^4+x^3+x+1
```

The same polynomial is reducible in \mathbb{Z}_5 but irreducible in \mathbb{Z}_2 .

Polynomials over Finite Fields

Polynomial equations and factorizations in finite fields can be different than over the rationals.

Examples from an XMAPLE session:

```
factor(x^6-1); # over the rationals  
      (x-1)(x+1)(x^2+x+1)(x^2-x+1)  
Factor(x^6-1) mod 7; # over Z7  
      (x+1)(x+3)(x+2)(4+x)(x+5)(x+6)  
factor(x^4+x^2+x+1); # over the rationals  
      x^4+x^2+x+1  
Factor(x^4+x^2+x+1) mod 2; # over Z2  
      (x+1)(x^3+x^2+1)
```

Implementing $GF(p^k)$ arithmetic

Theorem: Let $f(x)$ be an irreducible polynomial of degree k over \mathbb{Z}_p .

The finite field $GF(p^k)$ can be realized as the set of degree $k-1$ polynomials over \mathbb{Z}_p , with addition and multiplication done modulo $f(x)$.

Example: Implementing $GF(2^k)$

By the theorem the finite field $GF(2^5)$ can be realized as the set of degree 4 polynomials over Z_2 , with addition and multiplication done modulo the irreducible polynomial $f(x)=x^5+x^4+x^3+x+1$.

The coefficients of polynomials over Z_2 are 0 or 1. So a degree k polynomial can be written down by $k+1$ bits. For example, with $k=4$:

$$x^3+x+1 \leftrightarrow (0,1,0,1,1)$$

$$x^4+x^3+x+1 \leftrightarrow (1,1,0,1,1)$$

Implementing $GF(2^k)$

Multiplication: Polynomial multiplication, and then remainder modulo the defining polynomial $f(x)$:

```
> g(x) := (x^4+x^3+x+1) * (x^3+x+1);
      g(x) := (x^4+x^3+x+1)(x^3+x+1)
> f(x) := x^5+x^4+x^3+x+1;
      f(x) := x^5+x^4+x^3+x+1
> rem(g(x), f(x), x);
      1+3x^4+x^3+2x
> % mod 2;
      1+x^4+x^3
```

(1,1,0,1,1) * (0,1,0,1,1) = (1,1,0,0,1)

For small size finite field, a lookup table is the most efficient method for implementing multiplication.

Implementing $GF(2^k)$

Addition: bit-wise XOR (since $1+1=0$)

$$\begin{array}{r} x^3+x+1 \quad (0,1,0,1,1) \\ + \\ x^4+x^3+x \quad (1,1,0,1,0) \\ \hline x^4 \quad +1 \quad (1,0,0,0,1) \end{array}$$

Implementing $GF(2^5)$ in XMAPLE

Irreducible polynomial

```
> G32 := GF(2, 5, x^5+x^4+x^3+x+1);
> a := G32[ConvertIn](x);
      a := x
> b := G32[^^](a, 8); # colon at end of
      statement suppresses printing
c := G32[^^](a, 9);
G32[ConvertOut](b); # canonical
representation, higher monomials to the left
G32[ConvertOut](c);
      x^3+x^2+x+1
      x^4+x^3+x^2+x
```

More GF(2⁵) Operations in XMAPLE

```

> d := G32[`+`](b,c);           Addition: b+c
   G32[ConvertOut](d);
                                x4 + 1
> G32[isPrimitiveElement](d);   test primitive element
                                true
> e:=G32[``^`](a,-1);           e <--inverse of a
   G32[ConvertOut](e);
                                x4 + x3 + x2 + 1
> G32[``*`](a,e);               Multiplication: a*e
                                1

> for i from 1 to 32 do
  f:= G32[``^`](a,i);
  print(f, G32[isPrimitiveElement](f))
end do;
                                x, true
                                x2, true
                                x3, true
                                x4, true
                                1 + x + x3 + x4, true
                                1 + x2 + x3, true
                                x + x3 + x4, true

```

Loop for
finding primitive
elements

Back to Symmetric Block Ciphers

out	in
DES	AES

Historic Note

DES (data encryption standard) is a symmetric block cipher using 64 bit blocks and a 56 bit key.

Developed at IBM, approved by the US government (1976) as a standard. Size of key (56 bits) was apparently small enough to allow the NSA (US national security agency) to break it exhaustively even back in 70's.

In the 90's it became clear that DES is too weak for contemporary hardware & algorithmics. (Best attack, Matsui "linear attack", requires only 2⁴³ known plaintext/ciphertext pairs.)

Historic Note (cont.)

The US government NIST (national inst. of standards and technology) announced a call for an advanced encryption standard in 1997.

This was an international open competition. Overall, 15 proposals were made and evaluated, and 6 were finalists. Out of those, a proposal named Rijndael, by Daemen and Rijmen (two Belgians) was chosen in February 2001.

AES - Advanced Encryption Standard

- Symmetric block cipher
- Key lengths: 128, 192, or 256 bits
- Approved US standard (2001)

AES Design Rationale

- Resistance to all known attacks.
- Speed and code compactness.
- Simplicity.

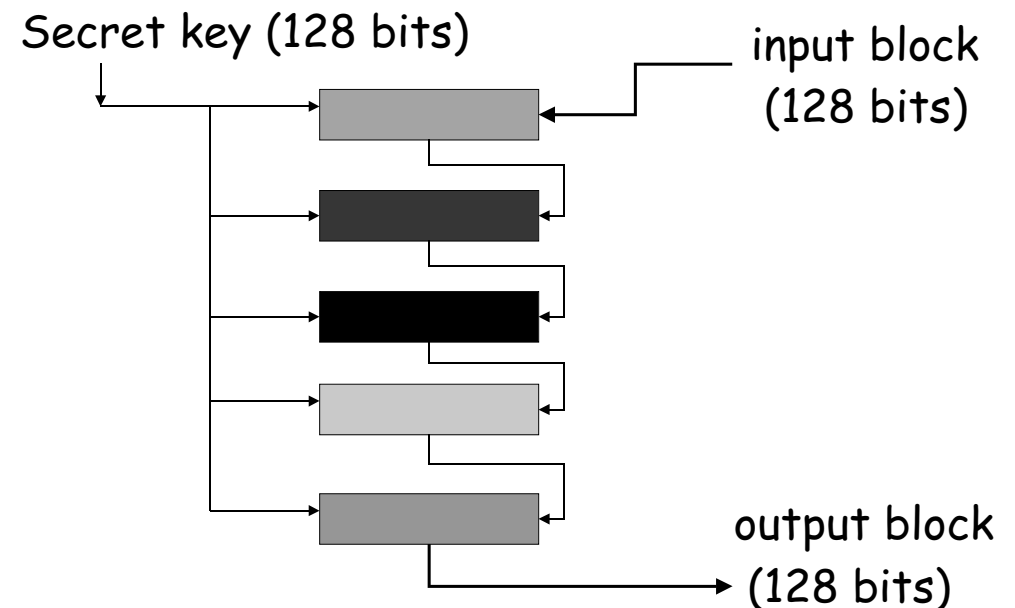
AES Specifications

- Input & output block length: 128 bits.
- State: 128 bits, arranged in a 4-by-4 matrix of bytes.

$A_{0,0}$	$A_{0,1}$	$A_{0,2}$	$A_{0,3}$
$A_{1,0}$	$A_{1,1}$	$A_{1,2}$	$A_{1,3}$
$A_{2,0}$	$A_{2,1}$	$A_{2,2}$	$A_{2,3}$
$A_{3,0}$	$A_{3,1}$	$A_{3,2}$	$A_{3,3}$

Each byte is viewed as an element in $GF(2^8)$

Encryption: Carried out in rounds



Rounds in AES

128 bits AES uses 10 rounds

- The secret key is expanded from 128 bits to 10 round keys, 128 bits each.
- Each round changes the state, then XORS the round key.

Each rounds complicates things a little.
Overall it seems infeasible to invert without the secret key (but easy given the key).

Substitution (S-Box)

Substitution operates on every Byte separately: $A_{i,j} \leftarrow A_{i,j}^{-1}$
(multiplicative inverse in $GF(2^8)$
which is highly non linear.)

If $A_{i,j} = 0$, don't change $A_{i,j}$.

Clearly, the substitution is invertible.

AES Specifications: One Round

Transform the state by applying:

$A_{0,0}$	$A_{0,1}$	$A_{0,2}$	$A_{0,3}$
$A_{1,0}$	$A_{1,1}$	$A_{1,2}$	$A_{1,3}$
$A_{2,0}$	$A_{2,1}$	$A_{2,2}$	$A_{2,3}$
$A_{3,0}$	$A_{3,1}$	$A_{3,2}$	$A_{3,3}$

1. Substitution.
2. Shift rows
3. Mix columns
4. XOR round key

Cyclic Shift of Rows

$A_{0,0}$	$A_{0,1}$	$A_{0,2}$	$A_{0,3}$
$A_{1,3}$	$A_{1,0}$	$A_{1,1}$	$A_{1,2}$
$A_{2,2}$	$A_{2,3}$	$A_{2,0}$	$A_{2,1}$
$A_{3,1}$	$A_{3,2}$	$A_{3,3}$	$A_{3,0}$

- no shift
- shift 1 position
- shift 2 positions
- shift 3 positions

Clearly, the shift is invertible.

More AES Specifications

- Expanding key to round keys
- Mixing columns

These items are intentionally left blank.

But details are not complicated - see Rijndael document (available on the course site) if curious.

Breaking AES

Breaking 1 or 2 rounds is easy.

It is not known how to break 5 rounds.

Breaking the full 10 rounds AES efficiently (say 1 year on existing hardware, or in less than 2^{128} operations) is considered impossible ! (a good, tough challenge...)