Cryptography
ECE5632 - Spring 2025

Lecture 6A

Dr. Farah Raad

Lecture Topic

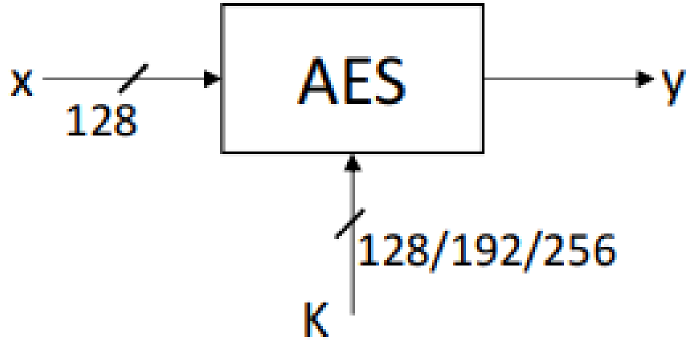
The Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES)

- AES is the most widely used symmetric cipher today.
- Found in every web browser, in banking machines, WiFi routers, etc ..

The requirements for all AES candidate submissions were:

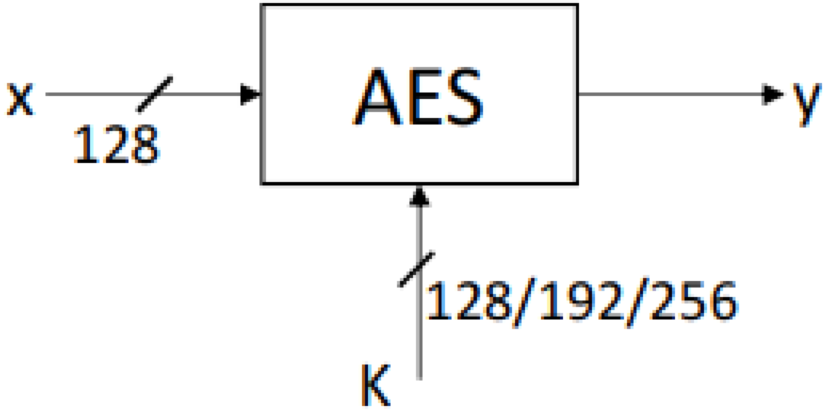
- Block cipher with **128-bit block size**
- **Three supported key lengths**: 128, 192 and 256 bit
- Security relative to other submitted algorithms
- **Efficiency** in software and hardware



The Advanced Encryption Standard (AES)

How does it work?

All internal operations of AES are based on **Finite Fields**.



Finite Fields (Galois Fields)

What's a **Field**?

Abstract (modern) algebra consists of three basic elements

1. Group
2. Ring
3. Field

1. Group

Group {G,+, −}: a set of elements, such that the following axioms are obeyed:

<u>A1. Closure:</u>

If a and b belong to G, then $a \circ b$ is also in G.

<u>A2. Associativity:</u>

$a \circ (b \circ c) = (a \circ b) \circ c$ for all a, b, c in G

<u>A3. Identity element:</u>

There is an element 0 in G such that $a \circ 0 = 0 \circ a = a$ for all a in G

<u>A4. Inverse element:</u>

For each a in G there is an element -a in G such that $a \circ (-a) = (-a) \circ a = 0$

<u>A5. Commutativity:</u>

$a \circ b = b \circ a$ for all a, b in G

Note:
the generic operator $\circ$ denotes either + or −

But we're interested in more than just +, −

2. Ring

Ring {R,+, −,×}: a set of elements such that the following axioms are obeyed:

A1~A5.

M1. Closure under multiplication:

If a and b belong to R, then ab is also in R

M2. Associativity of multiplication:

a(bc) = (ab)c for all a, b, c in R

M3. Distributive laws:

a(b + c) = ab + ac for all a, b, c in R

(a + b)c = ac + bc for all a, b, c in R

M4. Commutativity of multiplication:

ab = ba for all a, b in R

M5. Multiplicative identity:

There is an element 1 in R such that a1 = 1a = a for all a in R

M6. No zero divisors:

If a, b in R and ab = 0, then either a = 0 or b = 0

Still, we're interested in more than just +, −,×

3. Field

Field {F,+, −,×,()$^{-1}$}: a set of elements, such that the following axioms are obeyed:

<u>A1~A5</u>.

<u>M1~M6</u>.

<u>M7. Multiplicative inverse:</u>

For each a in F, except 0,
there is an element a^{-1} in F such that $aa^{-1}=(a^{-1})a=1$.

Finally! 

Simply, it's a set of numbers which we can add, subtract, multiply, and invert, that obey A1~A5 & M1~M7.

Example: Which of the following are Fields? $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$

Finite Fields (Galois Fields)

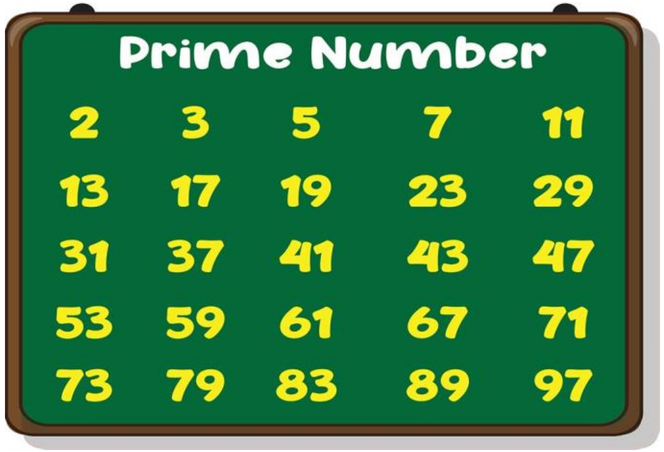
- In crypto, we almost always need finite sets.

m: positive integer

Theorem: A finite field only exists if it has p^m elements.

p: prime integer

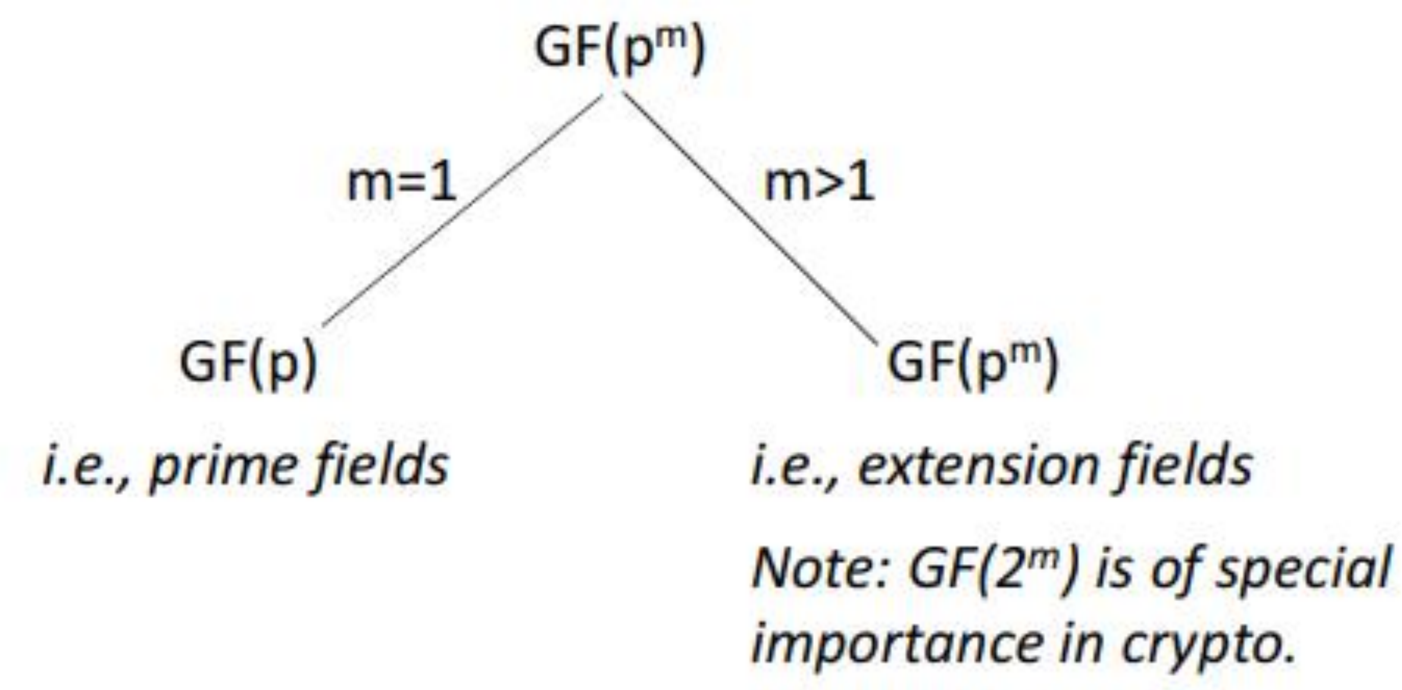
- **Order** or **cardinality** of the field: number of elements in GF.



Examples:

1) There's a finite field with 11 elements. GF(11)
2) There's a finite field with 81 elements. GF(81) = GF(3^4)
3) There's a finite field with 256 elements. GF(256) = GF(2^8) ← The Galois field specified in the AES standard.
4) Is the field with 12 elements a finite field?

Types of Finite Fields



Prime Field Arithmetic

The elements of a prime field GF(p) are the integers {0, 1, . . ., p−1}

a) Add, subtract, multiply:

$$a \circ b \equiv c \bmod p$$

Note:
the generic operator $\circ$ here denotes either $+$, $-$, or $\times$

b) Inversion:

$a \in GF(p)$; the inverse a^{-1} must satisfy $a \cdot a^{-1} \equiv 1 \bmod p$

a^{-1} can be computed using the extended Euclidian Algorithm.

Extension Field GF(2^m) Arithmetic

The elements of GF(2^m) are polynomials.

$a_{m-1}x^{m-1} + \ldots + a_1x + a_0 = A(x) \in GF(2^m)$

Coefficients $a_i \in GF(2) = \{0, 1\}$

Example:

$GF(2^3) = GF(8)$

$A(x) = a_2x^2 + a_1x + a_0 \quad = (a_2, a_1, a_0)$

$GF(2^3) = \{0, 1, x, x+1,$
$x^2, x^2+1, x^2+x,$
$x^2+x+1\}$

Extension Field GF(2^m) Arithmetic

a) Add and subtract in GF(2^m):

$$C(x) = A(x) \circ B(x) = \sum_{i=0}^{m-1} c_i x^i, \; ci \equiv ai + bi \bmod 2$$

Note:
the generic operator $\circ$ here denotes either $+, -$

Example: In GF(2^3), $A(x) = x^2 + x + 1$, $B(x) = x^2 + 1$
Compute $A(x) + B(x)$

$A(x) + B(x) = (1+1)x^2 + x + (1+1)$

$= 0x^2 + x + 0$

$= x \quad = A(x) - B(x)$

GF(2^3)= { $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ }

Note:
Addition and subtraction in GF(2^m) are the same operations.

Extension Field GF(2^m) Arithmetic

b) Multiplication in GF(2^m):

Example: In GF(2^3), $A(x) = x^2 + x + 1$, $B(x) = x^2 + 1$
Compute $A(x) \times B(x)$

GF(2^3)= { $0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$ }

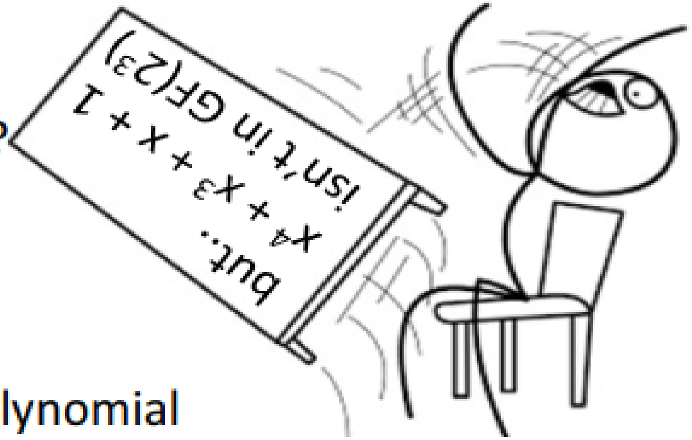
$$A(x) \times B(x) = (x^2 + x + 1)(x^2 + 1)$$

$$= x^4 + x^3 + x^2 + x^2 + x + 1$$

$$= x^4 + x^3 + (1+1)x^2 + x + 1$$

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

Simple..?



So, call this result $x^4 + x^3 + x + 1 = C'(x)$

Solution: Reduce C'(x) modulo a polynomial that behaves like a prime.
i.e., a polynomial that cannot be factored.
i.e., an irreducible polynomial.

In the next example..

Extension Field GF(2^m) Arithmetic

b) Multiplication in GF(2^m):

$$C(x) \equiv A(x) \times B(x) \bmod P(x)$$, where $P(x)$ is an irreducible polynomial.

Example: Given the irreducible polynomial for GF(2^3) $P(x) = x^3 + x + 1$
$A(x) = x^2 + x + 1$, $B(x) = x^2 + 1$
Compute $A(x) \times B(x) \bmod P(x)$

$A(x) \times B(x) = x^4 + x^3 + x + 1 = C'(x)$

$$
\begin{array}{r|l}
 & x + 1 \\ \hline
x^3 + x + 1 & x^4 + x^3 \qquad\quad + x + 1 \\
 & x^4 \qquad + x^2 + x \\ \cline{2-2}
 & \qquad x^3 + x^2 \qquad + 1 \\
 & \qquad x^3 \qquad + x + 1 \\ \cline{2-2}
 & \qquad\qquad x^2 + x \quad \equiv A(x) \times B(x) \bmod P(x) \equiv C(x)
\end{array}
$$

Extension Field GF(2^m) Arithmetic

Where did P(x) come from in the previous example??

Actually, for every finite field GF(2^m), there are several irreducible polynomials!

So, for a given finite field (e.g., GF(2^3)), the computation result depends on P(x).

So, multiplication can't be done unless the irreducible polynomial is specified.

It must be..

The AES standard specifies the irreducible polynomial:

$P(x) = x^8 + x^4 + x^3 + x + 1$

✓ *How to test whether a P(x) is reducible or not?*

https://www.youtube.com/watch?v=pHQ73N3n-ZU

What about $()^{-1}$?

Extension Field GF(2^m) Arithmetic

c) Inversion in GF(2^m):

The inverse $A^{-1}(x)$ of an element $A(x) \in GF(2^m)$ must satisfy:

$A(x) \times A^{-1}(x) \equiv 1 \bmod P(x)$

Extended Euclidian Algorithm.

Thank You!

See You next Lectures!!

Any Question?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt
Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451
Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg