Mathematical background: Galois Field (GF)

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres

José María de Fuentes García-Romero de Tejada

Lorena González Manzano

Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

OUTLINE

- 1. Mathematical background
  - Basic concepts
  - Inverse computation
  - Congruence equations
  - Galois Field
    - Definition
    - Operations

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 1. Mathematical background
  - Basic concepts
  - Inverse computation
  - Congruence equations
  - Galois Field
    - Definition
    - Operations

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

ÉVARISTE GALOIS (1811 – 1832)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

BRIEF INTRODUCTION TO GALOIS FIELDS

$(A,+,\cdot)$ with $A=Z_p$

$+ : A \times A \rightarrow A$

$a,b \rightarrow (a+b) \pmod p$

$\cdot : A \times A \rightarrow A$

$a,b \rightarrow (a \cdot b) \pmod p$

- GF(p) , p prime
- All nonzero elements of GF(p) have an inverse!
- Arithmetic in GF(p) is done modulo p

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

BRIEF INTRODUCTION TO GALOIS FIELDS

- We wish to define an encryption algorithm that operates on data of 8 bits at a time

  $(A,+,\cdot)$ with $A=Z_{256}$

- $(Z_{256}, +,\cdot)$ is not a field

- Let $A=Z_{251}$
  - It is a field but inefficient use of storage
  - $2^7 < 253 < 2^8$ for instance is not represented

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

BRIEF INTRODUCTION TO GALOIS FIELDS

- A: set of polynomials a(x) of degree n-1 or less with coefficients in Z_q (q prime)
  - $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots\cdots + a_1 x + a_0 \qquad a_i \in Z_q$
  - q^n polynomials in total
    - In AES: q = 2
  - a(x) are the remainders of dividing polynomials by p(x)
  - p(x) irreducible polynomial
  - $GF(q^n)$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

ADVANTAGES OF $GF(2^N)$ RESPECT TO GF(P)

- Simpler operations
  - There is no need to reduce modulo p(x) for + and –
  - · xtime operation
- The order of $GF(2^n)$ is greater than GF(p)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 1. Mathematical background
  - Basic concepts
  - Inverse computation
  - Congruence equations
  - Galois Field
    - Definition
    - Operations

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

ARITHMETIC IN $GF(2^N)$

- a(x) represented by its coefficients
  - $a(x) = a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots\cdots+a_1x+a_0$
  - $(a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$ – n bits

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

ARITHMETIC IN GF(Q^N)

- Addition $a(x) \in GF(q^n)$
  - c(x)=a(x)+b(x) mód p(x) ; $c_i = (a_i + b_i) \bmod q$
  - GF(2^n), c(x)= a_i XOR b_i
- Multiplication
  - c(x)=a(x)·b(x) mod p(x)
    - In AES: (A,+,·) = GF(2^8) with $p(x) = x^8 + x^4 + x^3 + x + 1$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

ADDITION AND SUBSTRACTION IN GF(2^N)

- $c_i = (a_i \pm b_i) \bmod 2 = a_i \oplus b_i$

- Ex. Let a=(10110) and b=(10101) in GF(2^5). Compute c=a+b:

$$c=(10110)\oplus(10101)= 00011$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

MULTIPLICATION IN GF(2^N)

- Ex. Let a=(101) in GF(2^3) and p(x)= (1011). Compute c=a·a:

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

MULTIPLICATION IN GF(2^N)

- Ex. Let a=(101) in GF(2^3) and p(x)= (1011). Compute c=a·a:
- $(x^2+1)(x^2+1) = x^4+x^2 + x^2+1 = x^4+1$
- $x^4 + 1$ | $x^3 + x + 1$

$$
\begin{array}{r|l}
x^4 + \qquad\qquad\qquad 1 & x^3 + x + 1 \\ \hline
x^4 + \quad + x^2 + x \qquad & x \\ \hline
x^2 + x + 1 &
\end{array}
$$

MULTIPLICATION IN GF(2^N)

$a(x) = x^2+1$ (101)

$$
\begin{array}{ccccc}
 & & 1 & 0 & 1 \\
 & & 1 & 0 & 1 \\
\hline
 & & 1 & 0 & 1 \\
1 & 0 & 1 & & \\
\hline
1 & 0 & 0 & 0 & 1
\end{array}
$$

$$
\begin{array}{l|l}
10001 & 1011 \\
\cline{2-2}
\underline{1011} & 10 \\
00111 & \\
\quad 111 = x^2+ x +1 &
\end{array}
$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

MULTIPLICATION IN GF(2^N)

- $p(x) = x^3+x+1 = (1011)$
- $x^3 \bmod p(x) = [p(x)-x^3] = x+1 = (011)$
- $a(x) = x^2+1$

$$x*a(x)= \begin{cases} (a_1\, a_0\, 0) & \text{if } a_2=0 \\ (a_1\, a_0\, 0) \oplus (011) & \text{if } a_2<>0 \end{cases}$$

- $a(x) \cdot a(x) = (x^2+1)\,(x^2+1) = x^2\,(x^2+1) + (x^2+1) =$

$= x\,(x^2+1)\,x + (x^2+1);\ \ ((010) \oplus (011))\,(010) \oplus (101)$

$= (001)\,(010) \oplus (101) = (010) \oplus (101) = (111);\quad x^2+x+1$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

COMPUTING INVERSES IN $GF(2^N)$

- $a(x)\ a^{-1}(x) = 1 \bmod p(x)$
- $p(x)$ is irreducible for all $a(x) \in GF(2^n)$, excluding $a(x)=0$
- $\Phi(p(x)) = 2^n - 1$
  - # elements of $GF(2^n)$ that are coprime with $p(x)$
- Euler's Theorem

  $a^{\Phi(p(x))} \bmod (p(x)) = 1$

  $a^{-1} = a^{\Phi(p(x)) - 1} \bmod (p(x))$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

COMPUTING INVERSES IN GF(2^N)

- Compute the inverse of $a(x)=(100)=x^2$ in GF(2^3) with $p(x)=x^3+x+1=(1011)$
- $\Phi(p(x)) = 2^n - 1 = 7;$
- $a^{-1} = (100)^{\Phi(p(x))-1} \bmod (p(x)) = (100)^6 \bmod (1011) =$

$= (x^2)^6 \bmod (p(x)) = x^{12} \bmod (p(x)) = x^2+x+1$

  – Dividing polynomials

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

COMPUTING INVERSES IN GF(2^N)

- Using xtime:
  - a-1 = $(100)^6$ mod (1011) = $(x^2)^6$ mod (x^3+x+1) =
  - = x x x x x x x x x x x^2 mod (x^3+x+1)
  - (010)(100) = (000) ⊕ (011) = 011 x^3 mod $(x^3+x+1) = x+1$
  - (010)(011) = (110) x^4 mod $(x^3+x+1) = x^2 + x$
  - (010)(110) = (100) ⊕ (011) = 111 x^5 mod $(x^3+x+1) = x^2 + x + 1$
  - (010)(111) = (110) ⊕ (011) = 101 x^6 mod $(x^3+x+1) = x^2 +1$
  - (010)(101) = (010) ⊕ (011) = 001 x^7 mod $(x^3+x+1) = 1$
  - (010)(001) = (010) x^8 mod $(x^3+x+1) = x$
  - (010)(010) = (100) x^9 mod $(x^3+x+1) = x^2$
  - (010)(100) = (000) ⊕ (011) = 011 x^{10} mod $(x^3+x+1) = x + 1$
  - (010)(011) = (110) x^{11} mod $(x^3+x+1) = x^2 + x$
  - (010)(110) = (100) ⊕ (011) = 111 x^{12} mod $(x^3+x+1) = x^2 + x + 1$

COMPUTING INVERSES IN GF(2^N)

- Extended Euclidean algorithm
- Given a(x) and p(x), compute b(x)

  a(x) b(x) =1 mod p(x)

$p(x) = c_1(x)\ a(x) + r_1x)$
$a(x) = c_2(x)\ r_1(x) + r_2(x)$
$r_1(x)= c_3\ (x)r_2(x)+ r_3\ (x)$
...

...
$r_{n-2} = c_n r_{n-1} + 1$
$r_{n-1} = c_{n+1} +0$

$1 = k_1(x)\ a(x) + k_2\ p(x)$

$1 = k_1(x)\ a(x)\ (\text{mod } p(x))$

$k_1= a^{-1}\ \ (\text{mód. } n) = b(x)$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid