ARITMETIKA MODULAR DAN FINITE FIELDS

KULIAH KRIPTOGRAFI DAN KEAMANAN JARINGAN

OUTLINE

- **Keterbagian dan algoritma pembagian**
- **Aritmetika modular**
- **Group, ring, field**
- **Aritmetika polinomial**

PENGGUNAAN

- **AES**
- **Kriptografi kurva elips**
- **Message authentication code: CMAC**
- **Skema enkripsi autentikasi GMC (Galois/Counter Mode)**

KETERBAGIAN

- **b membagi a jika a = mb, dengan a, b, m bilangan bulat.**
  - Notasi: b | a
  - b disebut pembagi dari a.
- **Properti dari keterbagian bilangan bulat:**
  - Jika a | 1 maka a = ± 1.
  - Jika a | b dan b | a maka a = ±b.
  - Sebarang b ≠ 0 membagi 0.
  - Jika a | b dan b | c maka a | c.
  - Jika b | g dan b | h maka b | (mg + nh) untuk sembarang bilangan bulat m dan n.
    - Misalkan g = b X g_1, h = b X h_1.
    - Maka mg + nh = $mbg_1 + nbh_1$ = b x ($mg_1 + nh_1$)

ALGORITMA PEMBAGIAN

- **Diberikan sebarang bilangan bulat (integer) positif n dan sebarang bilangan non-negatif a. Akan diperoleh integer quotient q dan integer remainder r yang memenuhi aturan:**
  - $a = qn + r , 0 \leq r \leq n; q = \lfloor a/n \rfloor$
  - r disebut residue.

GREATEST COMMON DIVISOR

- **Dua bilangan disebut relatif prima jika faktor persekutuannya hanya bilangan 1.**
  - Contoh: 8 dan 15 adalah relatif prima.
- **Greatest common divisor (faktor persekutuan terbesar) dari a dan b adalah integer paling besar yang membagi baik a maupun b.**
  - Notasi: gcd(a, b) atau fpb(a, b).
  - gcd(0, 0) = 0.
  - Harus bilangan positif → secara umum: gcd(a, b) = gcd(|a|, |b|).
  - gcd(a, 0) = |a|.

ALGORITMA EUCLID

- **Mencari gcd dengan algoritma Euclidean:**
  - Misalkan akan dicari gcd(a, b) dengan $a \geq b$.
  - Maka: $a = q_1 b + r_1, \ 0 \leq r_1 < b$. Jika $r_1 = 0$, maka $b \mid a$.
  - Karena $b > r_1$ maka: $b = q_2 r_1 + r_2, \ 0 \leq r_2 < r_1$.
  - Proses ini berulang sampai didapatkan remainder yang berupa 0 pada suatu langkah ke-(n+1):
    - $a = q_1 b + r_1, \ 0 < r_1 < b$.
    - $b = q_2 r_1 + r_2, \ 0 < r_2 < r_1$.
    - $r_1 = q_3 r_2 + r_3, \ 0 < r_3 < r_2$.
    - $r_2 = q_4 r_3 + r_4, \ 0 < r_4 < r_3$.
    - …
    - $r_{n-2} = q_n r_{n-1} + r_n, \ 0 < r_n < r_{n-1}$.
    - $r_{n-1} = q_{n+1} r_n + 0$
  - Maka: $d = \gcd(a, b) = r_n$

ARITMETIKA MODULAR

- **Jika a integer dan n integer positif, kita definisikan a mod n sebagai sisa dari a dibagi dengan n.**
  - n disebut modulus.
  - Contoh: 11 mod 7 = 4; -11 mod 7 = 3.
- **Dua integer a dan b disebut congruent modulo n jika a mod n = b mod n.**
  - Ditulis sebagai: $a \equiv b \pmod{n}$.
  - Contoh: $73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$
  - Jika $a \equiv 0 \pmod{n}$ maka $n \mid a$.
  - Properti kongruensi:
    - $a \equiv b \pmod{n}$ jika $n \mid (a-b)$.
    - $a \equiv b \pmod{n}$ mengakibatkan $b \equiv a \pmod{n}$.
    - $a \equiv b \pmod{n}$ dan $b \equiv c \pmod{n}$ mengakibatkan $a \equiv c \pmod{n}$

OPERASI ARITMETIKA MODULAR

- **Properti-properti:**
  - [(a mod n) + (b mod n)] mod n = (a + b) mod n.
    - Contoh: 11 mod 8 = 3; 15 mod 8 = 7
    - ((11 mod 8) + (15 mod 8)) mod 8 = 10 mod 8 = 2
    - (11 + 15) mod 8 = 26 mod 8 = 2
  - [(a mod n) - (b mod n)] mod n = (a - b) mod n.
    - ((11 mod 8) - (15 mod 8)) mod 8 = -4 mod 8 = 4
    - (11 - 15) mod 8 = -4 mod 8 = 4
  - [(a mod n) X (b mod n)] mod n = (a X b) mod n.
    - ((11 mod 8) x (15 mod 8)) mod 8 = 21 mod 8 = 5
    - (11 x 15) mod 8 = 165 mod 8 = 5
- **Operasi modulo pada perpangkatan:**
  - Contoh: berapa 11^7 mod 13?
  - $11^2 = 121 \equiv 4 \pmod{13}$
  - $11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
  - $11^7 = 11 \times 11^2 \times 11^4 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

KLAS RESIDU

- **Z_n adalah himpunan integer non-negatif kurang dari n: z_n = {0, 1, 2, …, (n-1)}.**
  - Z_n disebut himpunan residu atau clas residu (mod n).
  - Tiap integer dalam Z_n merepresentasikan klas residu.
  - Klas residu (mod n) dapat diberi label [0], [1], …, [n-1] dengan [r] = {a; a integer , $a \equiv r \pmod n$}
  - Contoh: salah satu klas residu (mod 4) adalah [1] ={…, -7, -3, 1, 5, 9, …}.

PROPERTI ARITMETIKA DALAM Z_N

- **Properti aritmetika modular untuk integer di dalam Z_n:**
  - Komutatif: $(w + x) \bmod n = (x + w) \bmod n$
    $(w \times x) \bmod n = (x \times w) \bmod n$
  - Asosiatif: $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
    $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
  - Distributif: $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
  - Identitas: $(0 + w) \bmod n = w \bmod n$; $(1 \times w) \bmod n = w \bmod n$
  - Invers aditif (-w): untuk setiap $w \in Z_n$ terdapat z sedemikian hingga $w + z \equiv 0 \bmod n$.
  - Jika $(a + b) \equiv (a + c) \pmod n$ maka $b \equiv c \pmod n$
  - Jika $(a \times b) \equiv (a \times c) \pmod n$ maka $b \equiv c \pmod n$ hanya jika a relatif prima terhadap n.

ALGORITMA EUCLID (2)

- **Basis: gcd(a, b) = gcd(b, a mod b)**
- **Maka algoritma tersebut dapat dinyatakan sebagai algoritma rekursif:**
  - Euclid(a, b)

    If (b = 0) then return a

    else return Euclid(b, a mod b);

GROUP

- **Group G:**
  - Notasi: {G, •}
  - Merupakan himpunan elemen dengan operasi biner yang dinotasikan dengan • yang menghubungkan setiap pasangan berurutan (a, b) dari elemen-elemen di G sedemikian hingga aksioma sbb berlaku:
    - Closure: jika a dan b berada di G, maka a • b juga di G.
    - Asosiatif: a• (b • c) = (a• b) • c
    - Elemen identitas: terdapat elemen e di G sedemikian hingga a • e = e • a = a untuk semua a di G.
    - Elemen invers: untuk setiap a di G, terdapat elemen a' di G sedemikian hingga a• a' = a' • a = e.
- **Finite group: group dengan jumlah elemen berhingga. Order group adalah jumlah elemen di grup.**
- **Infinite group: jumlah elemen tak berhingga.**

- **Group abelian: group yang memenuhi properti:**

  komutatif: $a \bullet b = b \bullet a$ untuk semua a, b di G

  - Contoh: himpunan bilangan bulat pada operasi penjumlahan.
- **Cyclic group:**
  - Dalam group:
    - $a^3 = a \bullet a \bullet a$
    - $a^0 = e$, e elemen identitas
    - $a^{-n} = (a')^n$, di mana a' adalah invers dari a di group.
  - Cyclic group: setiap elemen dari G adalah power dari a^k (k integer) dari suatu elemen a di G. Elemen a disebut generator di G.
  - Contoh: group penjumlahan bilangan bulat dengan elemen generator 1.

RING

- **Ring R:**
  - Notasi: {R, +, X}.
  - Adalah himpunan elemen dengan 2 operasi biner yang disebut penjumlahan dan perkalian sedemikian hingga untuk semua a, b, c di R aksioma berikut berlaku:
    - R merupakan grup abelian pada operasi penjumlahannya. Untuk grup aditif, elemen identitasnya adalah 0, sedangkan invers dari a adalah –a.
    - Closure pada perkalian: jika a dan b di R, maka ab juga di R.
    - Asosiatif dari perkalian: a(bc) = (ab)c untuk semua a, b, c di R.
    - Distributif: a(b+c) = ab + ac dan (a+b)c = ac + bc, a, b, c di R.
  - Ring adalah himpunan yang dapat dikenai operasi penjumlahan, pengurangan, dan perkalian tanpa harus meninggalkan himpunan tersebut.
  - Contoh: himpunan matriks bujur sangkar n dengan operasi penjumlahan dan perkalian.

- **Ring komutatif memenuhi aksioma:**
  - Komutatif pada perkalian: ab = ba untuk semua a, b di R.
- **Integral domain (domain integral): ring komutatif yang memenuhi:**
  - Identitas multiplikatif: Terdapat elemen 1 di R sedemikian hingga a1 = 1a = a untuk semua a di R.
  - Tidak ada pembagi 0: jika a, b di R dan ab = 0, maka a = 0 atau b = 0.
  - Contoh: himpunan bilangan bulat dengan operasi penjumlahan dan perkalian.

FIELD

- **Field:**
  - Notasi: {F, +, X}
  - Adalah himpunan elemen dengan 2 operasi biner penjumlahan dan perkalian sedemikian hingga aksioma sbb berlaku:
    - F adalah domain integral.
    - Invers multiplikatif: untuk setiap a di F, kecuali 0, terdapat elemen a^{-1} sedemikian hingga $aa^{-1} = a^{-1}a = 1$.
  - Field adalah himpunan di mana kita dapat melakukan operasi penjumlahan, pengurangan, perkalian, dan pembagian tanpa meninggalkan himpunan tersebut.
  - Contoh: himpunan bilangan rasional.

FINITE FIELD GF(p)

- **Finite field order p, dinotasikan dengan GF(p), adalah himpunan bilangan bulat Z_p= {0, 1, …, p – 1} dengan operasi modulo p.**
  - GF : Galois Field
- **Z_p = {0, 1, …, p-1} dengan aritmetika pada operasi modulo merupakan ring komutatif.**
  - Z_p adalah grup abelian :
    - Closure: (w + x) mod p $\in Z_p$
    - Asosiatif: [(w + x) + y] mod p = [w + (x + y)] mod p
    - Komutatif: (w + x) mod p = (x + w) mod p
    - Identitas: (0 + w) mod p = w mod p
    - Invers aditif (-w): untuk semua w $\in Z_p$ terdapat z sedemikian hingga w + z ≡ 0 mod p.
  - Z_p adalah ring komutatif :
    - Closure: (w X x) mod p $\in Z_p$
    - Asosiatif: [(w X x) X y] mod p = [w X (x X y)] mod p
    - Distributif: [w X (x + y)] mod p = [(w X x) + (w X y)] mod p
    - Komutatif: (w X x) mod p = (x X w) mod p

- **Suatu integer dalam Z_p memiliki invers multiplikatif jika dan hanya jika integer tersebut relatif prima terhadap p.**
  - Invers multiplikatif (w^{-1}): untuk semua $w \in Z_p$, $w \neq 0$, terdapat $z \in Z_p$ sedemikian hingga $w \times z \equiv 1 \bmod p$.

- **Contoh: finite filed GF(2)**

penjumlahan

+	0	1
0	0	1
1	1	0

perkalian

x	0	1
0	0	0
1	0	1

invers

w	-w	w^{-1}
0	0	-
1	1	1

  - Penjumlahan ekuivalen dengan XOR.
  - Perkalian ekuivalen dengan AND.

- **Contoh : GF(7)**

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

w	-w	w^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

FINITE FIELD GF(2^N)

- **Misalkan suatu algoritma enkripsi beroperasi pada 8 bit.**
  - Range: 0 – 255
  - Tetapi 256 bukan prima → aritmetika modulo 256 bukan merupakan field.
  - Bilangan prima terdekat: 251 → integer 251 sampai 255 tidak digunakan→ penyimpanan tidak efisien.
- **Penggunaan blok 3-bit :**
  - Aritmetika modulo 8 (Z_8) didefinisikan.
  - Tetapi kemunculan bilangan tidak nol pada tabel perkalian tidak merata.
    - Hanya empat kemunculan untuk 3, tetapi 12 kemunculan untuk 4.

tabel perkalian Z_8

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$GF(2^3)$

- **Penjumlahan dan perkalian 2^3**
  - Tabel penjumlahan dan perkalian simetris pada diagonal utama → sifat komutatif
  - Semua elemen tidak nol memiliki invers multiplikatif.
  - Memenuhi syarat finite field → $GF(2^{3)}$

- **Tabel penjumlahan pada GF(2^3)**

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

- **Tabel perkalian pada GF(2^3)**

		000	001	010	011	100	101	110	111
	x	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	5	7
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

ARITMETIKA POLINOMIAL

- **Polinomial order n ($n \geq 0$) :**
  - $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = \sum_{i=0}^{n} a_i x^i$
  - $f(x) = \sum_{i=0}^{n} a_i x^i$; $g(x) = \sum_{i=0}^{m} a_i x^i$
- **Operasi:**
  - Penjumlahan
  - Pengurangan
  - Perkalian
  - Pembagian
- **Contoh: $f(x) = x^3 + x^2 + 2$; $g(x) = x^2 - x + 1$**
  - $f(x) + g(x) = ?$
  - $f(x) - g(x) = ?$
  - $f(x) \times g(x) = ?$
  - $f(x) / g(x) = ?$

- **Polinomial pada field F disebut irreducible jika dan hanya jika f(x) tidak dapat diekspresikan sebagai hasil kali dari 2 polinomial dengan derajat lebih kecil dari derajat f(x) → polinomial prima.**
  - Contoh : $f(x) = x^3 + x + 1$ merupakan polinomial irreducible.

ARITMETIKA POLINOMIAL MODULAR PADA (2^N)

- **Penjumlahan sama dengan operasi XOR.**
- **Penjumlahan dan pengurangan ekuivalen pada mod 2 → 1 + 1 = 1 – 1 = 0; 1 + 0 = 1 – 0 = 1; 0 + 1 = 0 – 1 = 1**
- **Jika perkalian menghasilkan polinomial dengan derajat lebih besar daripada n – 1, maka polinomial direduksi dengan melakukan operasi modulo dengan suatu irreducible polynomial m(x) dengan derajat n.**
  - Kita bagi dengan m(x) dan menyimpan sisanya.
  - Untuk suatu polinomial f(x), remainder/sisa diekspresikan sebagai r (x) = f(x) mod m(x).
- **Contoh : irreducible polynomial derajat 3 adalah ($x^3 + x^2 + 1$) dan ($x^3 + x + 1$).**

- **Tabel penjumlahan pada GF(2^3)**

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

- **Tabel perkalian pada GF(2^3)**

		000	001	010	011	100	101	110	111
	x	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	5	7
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

POLINOMIAL DI AES

- **Menggunakan GF(2^8).**
- **Irreducible polynomial: $m(x) = x^8 + x^4 + x^3 + x + 1$.**
- **Contoh:**
  - $f(x) = x^6 + x^4 + x^2 + x + 1$
  - $g(x) = x^7 + x + 1$
  - $f(x) + g(x) = x^7 + x^6 + x^4 + x^2$
  - $f(x) \times g(x) = (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$
  - $x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) / (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + 1$
- Maka: $f(x) + g(x) \mod m(x) = x^7 + x^6 + 1$

LATIHAN

- **Buatlah tabel penjumlahan dan perkalian untuk GF(2^4) dengan $m(x) = x^4 + x + 1$.**