Introducere în teoria numerelor din criptografie

Curs SMD 2020

Prof. matematică Bâcă Ana-Maria

Facultatea de Automatică și Calculatoare
Universitatea Politehnica București

30 aprilie 2020

1 Istorie

2 Noțiuni introductive

3 Aritmetică. Congruențe

4 Teoreme importante (Euler, Fermat, Wilson, numere prime)

5 Cum folosim aritmetica modulară în criptare

6 Problema logaritmului discret. Diffie-Hellman

7 Criptare simetrică: AES

8 Criptare asimetrică: RSA

9 Concluzii

10 Quiz

Istorie

- Enigma - era mașină de criptare mecanică
- 1947 - la Bell AT&T este inventat tranzistorul
- 1951 - compania Feranti pornește producția calculatoarelor
- 1959 - apar circuitele integrate

Istorie (cont.)

- 1973 - Biroul American pentru Standarde a anunțat că așteaptă propuneri pentru sistem standard de criptare
- 1976 - versiune pe 56 biți a DES (Lucifer) - cu foarte multe chei - criptare simetrică
- Problemă: cum distribuim cheile?
- Anii '70: curieri (COMSEC), apelurile telefonice erau evitate

Scenariu de transfer chei (criptare asimetrică)

- Alice vrea să îi trimită un mesaj secret lui Bob
- Alice pune mesajul într-o cutie de fier, o încuie și o trimite lui Bob
- Bob când primește cutia o închide și el cu lacătul lui și o trimite înapoi la Alice
- Când Alice primește cutia are două lacăte. Alice scoate lacătul ei și o trimite înapoi la Bob
- Bob a primit acum cutia cu lacătul lui deci o poate deschide și citi mesajul

Grupuri

- Un grup G este o mulțime, împreună cu o operație binară pe G, notată: $\cdot : G \times G \to G, (x, y) \to x \cdot y$, astfel încât:
  - este îndeplinită asociativitatea
  - există element neutru
  - se pot inversa elementele
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$.
- $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}, \mathcal{U}(\mathbb{Z}_n)$.
- Ordinul unui element a al unui grup $(G, \cdot)$: $a^k = a \cdot a \cdot \ldots \cdot a = 1$
- Grup ciclic: $ord(a) = |G|$

Inele. Corpuri

- Un inel R este o mulțime, împreună cu două operații binare pe G, notate: $+ : R \times R \to R$, $\cdot : R \times R \to R$, astfel încât au $(R, +)$ e grup abelian, $(R, \cdot)$ e monoid și este îndeplinită distributivitatea $\cdot$ față de $+$
- R este corp: $\forall x \in R \setminus \{0\}$, x este inversabil în raport cu operația $\cdot$
- Exemplu corpuri: $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_n, +, \cdot), n$ prim
- Orice corp este inel integru (domeniu de integritate).

Aritmetică. Congruențe

Pentru o funcție $f : \mathbb{R} \to \mathbb{R}$ trebuie:

- Calculul $y = f(x)$ să fie simplu computațional
- Calculul inversei $x = f^{-1}(y)$ sa fie nefezabil chiar și cu un supercomputer

Un răspuns oferit de matemtică este aritmetica modulară

Aritmetica modulară - analogie cu ceasul

- Mulțimea $\mathbb{Z}_{12}$ ne-o putem imagina ca pe un cadran de ceas cu numere de la 0 la 11
- Dacă acum e ora 9 și avem întâlnire peste 8 ore atunci întâlnirea este la ora 5: $9 + 8 \pmod{12}$
- Funcțiile în aritmetica modulară au comportament neregulat tind să fie neinversabile
- Exemplu: Cum rezolvăm ușor ecuația $3^x \pmod 7 = 1$

Aritmetică. Congruențe

- Teorema împărțirii cu rest: $b = aq + r, 0 \leq r < |a|$
- Numerele a și b sunt congruente modulo m dacă $m \mid a - b$: $a \equiv b \pmod{m}$
- Prin intermediul numărului m s-a introdus pe $\mathbb{Z}$ o relație binară numită relație de congruență.
- Există o infinitate de numere prime
- Goldbach: Orice număr întreg pozitiv par $n, n \geq 2$ poate fi scris ca suma a două numere prime
- Mersenne: Există o infinitate de numere prime de forma $2^n - 1$. Dacă $2^n - 1$ este prim, atunci n este prim

Găsirea cmmdc - Algoritmul extins al lui Euclid

Input: Fie r_0 și r_1 întregi pozitivi cu $r_0 > r_1$.
Output: (r_0, r_1) = c.m.m.d.c , unde $(r_0, r_1) = s \cdot r_0 + t \cdot r_1$.
Pas inițial:

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$i = 1$$

Găsirea cmmdc - Algoritmul extins al lui Euclid

WHILE $r_i \neq 0$

$$i = i + 1$$
$$r_i = r_{i-2} \pmod{r_{i-1}}; q_{i-1} = (r_{i-2} - r_i)/r_{i-1};$$
$$s_i = s_{i-2} - q_{i_1} \cdot s_{i-1}; t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$$

RETURN

$$(r_0, r_1) = r_{i-1}; s = s_{i-1}; t = t_{i-1}$$

Utilitate

Algoritmul extins al lui Euclid ne permite să calculăm inversele elementelor modulo m

Funcția ϕ a lui Euler

- Fie $m \geq 1$. Atunci $\phi(m)$ este numărul întregilor pozitivi $\leq m$ și primi cu m. $\phi(m)$ se numește funcția lui Euler.
- Exemplu: Fie $m = 240$. Atunci $m = 2^4 \cdot 3 \cdot 5 = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3}$.
$\Rightarrow \phi(m) = (2^4 - 2^3) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = 8 \cdot 2 \cdot 4 = 64$.
- Există 64 de numere prime cu 240, iar funcția lui Euler este cea mai rapidă metodă.
- **Teorema lui Euler:** Dacă $m \geq 1$ și $(a, m) = 1$, atunci $a^{\phi(m)} \equiv 1 \pmod{m}$.

Teorema lui Fermat

- Dacă $m \geq 1$ și $(a, m) = 1$, atunci $a^{\phi(m)} \equiv 1 \pmod{m}$
- Fie $p = 7$ și $a = 2$. Atunci inversul lui a este $a^{p-2} = 2^5 = 32 \equiv 4 \pmod{7}$
- Verificăm rezultatul: $2 \cdot 4 \equiv 1 \pmod{7}$.

Rezolvarea înmulțirilor în aritmetica modulară

- $3x \equiv 2 \pmod 7$
- Congruența se verifică pentru $x_0 = 3$ deoarece $3 \cdot 3 - 2 \vdots 7$.
- Numerele $10, 17, -4$ verifică de asemenea congruența. Toate aceste numere se află în clasa $\widehat{3}$ din $\mathbb{Z}_7$.

Rezolvarea înmulțirilor în aritmetica modulară (cont.)

- Congruența $3x \equiv 2 \pmod 6$ nu are soluție.
- Dacă $3x_0 \equiv 2 \pmod 6$, atunci $6 \mid 3x_0 - 2$,
- Deci $3 \mid 3x_0 - 2$, adică se obține contradicția $3 \mid 2$.

Teoremă

Congruența $ax \equiv b \pmod m$ are soluție dacă și numai dacă $d \mid b$, unde $d = (a, m)$. Dacă $d \mid b$, atunci congruența are d soluții.

Înmulțirea în aritmetica modulo e ușoară

- Teoremă: Dacă $(a, m) = 1$, atunci congruența $ax \equiv b \pmod{m}$ este verificată de $x_0 = ba^{\phi(m)-1}$.
- $35x \equiv 14 \pmod{28}$. $d = (35, 28) = 7 \Rightarrow 7$ soluții.
- $35x \equiv 14 \pmod{28} | : 7 \rightarrow 5x \equiv 2 \pmod{4}$.
- $2, 6, 10, 14, 18, 22, 26.$ (cele 7 soluții ale congruenței)

Cheile în criptare sunt numere prime

- Consecința observațiilor de mai sus este că avem nevoie de lucru cu chei în $\mathbb{Z}_p$ cu p număr prim
- Generator pseudorandom de chei numere prime folosește teorema următoare: Există o infinitate de numere prime de forma $4k+1, 4k+3, 6k+1, 6k+5$
- Cum pot afla că un număr e prim fără a apela la factorizare? Teorema lui Wilson spune: Dacă p este prim, atunci $(p-1)! \equiv -1 \pmod{p}$.

Și pentru că înmulțirea e ușoară: Problema logaritmului discret

- Fie grupul $\mathbb{Z}_{47}^*$ care are ordinul 46.
- Elementul $a = 5$ este generator al grupului. Pentru $b = 41$ problema logaritmului discret pentru este: găsiți x astfel încât $5^x \equiv 41 \pmod{47}$.
- Prin încercări repetate ale valorilor lui x găsim soluția $x = 15$.

Algoritmul Diffie-Hellman

- Alice vrea să trimită mesajul x, calculează $X = a^x \pmod p$ și îl trimite lui Bob
- Bob vrea să trimită mesajul y, calculează $Y = a^y \pmod p$ și îl trimite lui Alice
- Alice și Bob determină cheia calculând X^y și Y^x
- Exemplul din slide-ul anterior $a = 5, p = 47, X = 41, Y = 31$. Eve interceptează aceste numere și trebuie să rezolve sistemul de ecuații:

$$5^x \equiv 41 \pmod{47}$$
$$5^y \equiv 31 \pmod{47}$$

- Eve are doar opțiunea încercărilor repetate

Corpuri finite

- Un corp finit cu p^n elemente se mai numeste și corp Galois
- Se notează $GF(p^n)$ sau F_{p^n}, unde $p, n \in \mathbb{N}, p$ prim.
- În criptografie lucrăm cu corpuri finite (cu un număr finit de elemente) - corpuri Galois.
- Numărul elementului se numește ordinul corpului.

Corpuri finite (cont.)

- $GF(2)$ - cel mai mic corp finit (poartă XOR, poartă AND)
- Extinderea $GF(2^m)$. Operații folosite în AES:
  - Adunare modulo m
  - Înmulțirea polinoamelor
  - Inversarea polinoamelor
- Cheia privată se obține folosind Diffie-Hellman
- AES-256: $GF(2^8)$. Corpul acesta reprezintă cea mai bună alegere deoarece fiecare element al său poate fi considerat echivalentul unui byte.

Polinoame ireductibile

- În fiecare corp $GF(2^m)$ avem nevoie de un polinom ireductibil $P(x)$ de grad m cu coeficienți în $GF(2)$
- Pentru AES, polinomul ireductibil este $P(x) = x^8 + x^4 + x^3 + x + 1$

Criptarea RSA - ssh-keygen (cont.)

RSA Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key: $k_{pr} = (d)$

1. Choose two large primes p and q.
2. Compute $n = p \cdot q$.
3. Compute $\Phi(n) = (p-1)(q-1)$.
4. Select the public exponent $e \in \{1, 2, \ldots, \Phi(n) - 1\}$ such that

$$\gcd(e, \Phi(n)) = 1.$$

5. Compute the private key d such that

$$d \cdot e \equiv \bmod \Phi(n)$$

Criptarea RSA - ssh-keygen (cont.)

Alice		**Bob**
message $x = 4$		1. choose $p = 3$ and $q = 11$ 2. $n = p \cdot q = 33$ 3. $\Phi(n) = (3-1)(11-1) = 20$ 4. choose $e = 3$ 5. $d \equiv e^{-1} \equiv 7 \bmod 20$
	$\xleftarrow{k_{pub}=(33,3)}$	
$y = x^e \equiv 4^3 \equiv 31 \bmod 33$		
	$\xrightarrow{y=31}$	
		$y^d = 31^7 \equiv 4 = x \bmod 33$

Note that the private and public exponents fulfill the condition $e \cdot d = 3 \cdot 7 \equiv 1 \bmod \Phi(n)$.

Criptarea RSA - ssh-keygen (cont.)

- Condiția $gcd(e, \phi(n)) = 1$ ne garantează că inversul lui e (mod $\phi(n)$) există, astfel încât întotdeauna există o cheie privată d
- **Vulnerabilitate RSA**: numere prime mici, putem găsi un factor comun între două chei publice folosind algoritmul extins al lui Euclid pentru k_{pub} `https://eprint.iacr.org/2016/515.pdf`

În loc de concluzie - Vreau să devin hacker

Criptare simetrică: AES

- Corpuri finite. Corpuri Galois
- Operații cu polinoame
- Congruențe și aritmetică modulară cu polinoame

Criptare asimetrică: RSA

- Congruențe și aritmetică modulară cu numere în $\mathbb{Z}_p$, numere prime
- Teorema lui Euler, Fermat
- Algoritmul Extins al lui Euclid
- Problema logaritmului discret în aritmetică modulară

Quiz

- Fie cheia publică (n, e), $n = pq$ cu $p = 13, q = 7$ și $e = 5$. Determinați cheia privată d, folosind algoritmul lui Euclid.