Informatika biztonság alapjai 2. gyakorlat

Oláh Norbert

2022.

Tartalom

Helyettesítéses titkosítás

- Caesar titkosítás
  - nyílt szöveg (m)
  - kulcs (k)
  - titkosított szöveg $c = (m + k) mod\ 26 \rightarrow$ angol abc
  - visszfejtett szöveg $m = (c - k) mod\ 26$
- Kulcsszavas Caesar titkosítás
  - nyílt szöveg (m)
  - kulcs (k=8 security)
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
    O P Q V X Y Z S E C U R I T Y A B D F G H J K L M N
  - az eltolásos ábécéhez képest, hogy lényegesen több (n!, ahol n az ábécé hossza) variációja van
  - puszta rotációval nem lehet feltörni

Affin titkosítás

- Betűnkénti titkosítás
- A kulcs egy számpár K=(a,b) → LNKO(a,26)=1
- $c = (a * m + b) mod\ 26$
- $m = (a_1 * c - a_1 * b) mod\ 26$ ahol $a_1 * a = 1 mod\ 26$

Euklideszi algoritmus

80	50	30	20	**10**	0
-	1	1	1	2	

(845,68) LNKO?

Euklideszi algoritmus

845	68	29	10	9	**1**	0
-	12	2	2	1	9	

Így a két szám relatív prím, azaz:$(845, 68) = 1$

Euklideszi algoritmus pszeudó kód

- Euklidesz(a, b, d)
- $d \leftarrow a$
- If($b \neq 0$)
- Then Euklidesz($b, a \ mod \ b, d$)
- Return (d)

Kibővített Euklideszi algoritmus

Az a és b két egész szám legnagyobb közös osztója $x, y \in Z$ számokkal kifejezhető a következő alakban:

$(a, b) = a * x + b * y$

Mindig!

$x_0 = 1\ x_1 = 0$

$y_0 = 0\ y_1 = 1$

Képlet:

$x_{i+1} = x_i * q_i + x_{i-1}$

$y_{i+1} = y_i * q_i + y_{i-1}$

$x = (-1)^n * x_n$

$y = (-1)^{n+1} * y_n$

Kibővített Euklideszi algoritmus 1 példa

k	0	1	2	-
r_k	280	3	1	0
q_k	-	93	3	
x_k	1	0	1	
y_k	0	1	93	

$(-1)^2$ és $(-1)^{2+1}$

1=280*1+3*-93

Kibővített Euklideszi algoritmus 2 példa

k	0	1	2	3	4	
r_k	544	119	68	51	17	0
q_k	-	4	1	1	3	
x_k	1	0	1	1	2	
y_k	0	1	4	5	9	

$(-1)^4$ és $(-1)^{4+1}$

17=544*2+119*-9

Kibővített Euklideszi algoritmus pszeudó kód

- KibővítettEuklidesz(a, b, d, x, y)
- $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$, $s \leftarrow 1$
- While $(b \neq 0)$
- $r \leftarrow a \ mod \ b$, $q \leftarrow a \ div \ b$
- $a \leftarrow b$, $b \leftarrow r$
- $x \leftarrow x_1$, $y \leftarrow y_1$
- $x_1 \leftarrow q * x_1 + x_0$, $y_1 \leftarrow q * y_1 + y_0$
- $x_0 \leftarrow x$, $y_0 \leftarrow y$
- $s \leftarrow -s$
- End While
- $x \leftarrow s * x_0$, $y \leftarrow -y_0$
- $(d, x, y) \leftarrow (a, x, y)$
- Return (d, x, y)

Gyorshatványozás

Az alábbi módszer alkalmazásával viszonylag kevés művelet elvégzésével megkapjuk a^b modulo m értékét, ahol a egész szám, b 1-nél nagyobb egész, m pozitív egész.

Algoritmus:

1. lépés: A kitevőt felírjuk 2 hatványainak összegeként:
$b = 2^{b_1} + 2^{b_2} + ... + 2^{b_r}$

2. lépés: ismételt négyzetre emeléssel számoljuk ki a következő értékeket: $a^{2^0}, a^{2^1}, ...a^{2^r}$

$a^{2^{k+1}} = a^{2^k * 2} = (g^{2^k})^2$

3. lépés: megkapjuk a keresett hatványt:

$a^b = a^{2^{b_1}} * a^{2^{b_2}} * ... * a^{2^{b_r}} \pmod{m}$

Példa

$6^{73} \pmod{100}$

$73 = 2^6 + 2^3 + 2^0$

$6^{2^0} \equiv 6 \pmod{100}$
$6^{2^1} \equiv 36 \pmod{100}$
$6^{2^2} \equiv 96 \pmod{100}$
$6^{2^3} \equiv 16 \pmod{100}$
$6^{2^4} \equiv 56 \pmod{100}$
$6^{2^5} \equiv 36 \pmod{100}$
$6^{2^6} \equiv 96 \pmod{100}$

$6^{73} = 6^{2^6} * 6^{2^3} * 6^{2^0} = 99 * 16 * 6 \equiv 16 \pmod{100}$

Feladat

$129^{97} \pmod{171}$

Feladat

$129^{97} \pmod{171}$

$97 = 2^6 + 2^5 + 2^0$

$129^{2^0} \equiv 129 \pmod{171}$
$129^{2^1} \equiv 54 \pmod{171}$
$129^{2^2} \equiv 9 \pmod{171}$
$129^{2^3} \equiv 81 \pmod{171}$
$129^{2^4} \equiv 63 \pmod{171}$
$129^{2^5} \equiv 36 \pmod{171}$
$129^{2^6} \equiv 99 \pmod{171}$

$129^{97} = 129^{2^6} * 129^{2^5} * 129^{2^0} = 99 * 36 * 129 \equiv 108 \pmod{171}$

Gyorshatványozás pszeudó kód

- Gyorshatvany($alap$, exp, mod)
- $alap = alap\%mod$,
- if($exp == 0$)
- return 0;
- else if($exp == 1$)
- return alap;
- else if($exp\%2 == 0$)
- return Gyorshatvany($alap * alap\%mod$, $exp/2$, mod);
- else
- return alap * Gyorshatvany($alap$, exp – 1, mod) $\%mod$;

Maradékosztályok

Ha $a \in Z$, akkor az a-val kongruens (mod m) egész számok halmazát az a által reprezentált (mod m) maradékosztálynak nevezzük.
Jelölés $(a)_m$
Z_n olyan halmaz melynek elemei maradékosztályok
Z_6=$(0)_6, (1)_6, (2)_6, (3)_6, (4)_6, (5)_6,$

Maradékosztályok tulajdonságok

- $(a)_m + (b)_m = (a + b)_m$
- $(a)_m * (b)_m = (ab)_m$
- bármely két halmazra elvégzünk egy adott műveletet akkor a halmazon belül marad
- Példák:
  $(2)_6 + (5)_6 = (2 + 5)_6 = 1_6$ $(3)_6 + (3)_6 = 0_6$ $(4)_6 + (5)_6 = 3_6$
  $(2)_6 * (5)_6 = 4_6$
- Algebrai struktúrát alkotnak.

Algebrai struktúrák

Adott egy $S = (x, y, z...)$ halmaz és ebben a halmazban definiálva van egy művelet. (általában összeadás és szorzás)

- félcsoport
- csoport
- Ábel- csoport
- gyűrű
- test

Algebrai struktúrák jellemző +, ·

- Asszociatív
  A maradék osztályok halmaza megörökli az egész számok asszocivatív tulajdonságát.
  Példa: $(xoy)oz = xo(yoz)$.
- Kommutatív
  A maradék osztályok halmaza megörökli az egész számok kommutativítás tulajdonságát.
  Példa: $xoy = yox$.
  Az összeadás is és a szorzás is kommutatív az egész számok körében.

Algebrai struktúrák jellemző +, ·

- J neutrális elem (egységelem)
  Az S -nek valamely *e* elemét egységelemnek vagy neutrális elemnek nevezzük, ha bármely $x \in S$ esetén: e o x = x o e = x
  + $(0)_m$ neutrális elem vagyis $(a)_m+(b)_m=(0)_m$
  · $(1)_m$ a neutrális elem vagyis $(a)_m \cdot (b)_m=(1)_m$
- J inverzek
  Ha S -ben létezik e egységelem, és ha az x elemhez létezik olyan y elem, hogy
  x o y = y o x = e,
  akkor y -t az x inverzének nevezzük.
  A valós számok halmazában 2 inverze 1/2.

Algebrai struktúrák jellemző +, ·

- Disztributivítás
  A maradék osztályok halmaza megörökli az egész számok disztributív tulajdonságát.
  $x(y + z) = xy + xz$
  és
  $(y + z)x = yx + zx$
  Az egész számok körében a szorzás disztributív az összeadásra nézve.

Egy S = x, y, . . . halmazt algebrai struktúrának nevezzük, ha definiálva van benne legalább egy művelet.

Csoportok

- Félcsoport
  Egy S halmaz félcsoport ha, definiálva van benne az **asszociatív** tulajdonság.
- Csoport
  Egy S halmaz csoport ha, definiálva van benne az **asszociatív** tulajdonság, valamint az létezik **neutrális elem** vagy **egységelem**, és minden elemnek létezik az **inverze**.
- Abel csoport
  Egy S halmaz Abel csoport ha, definiálva van benne az **asszociatív és kommutatív** tulajdonság, valamint az létezik **neutrális elem** vagy **egységelem**, és minden elemnek létezik az **inverze**.

Csoportok

- gyűrű

Gyűrű	(Z_m alaphalmaz;+)	(Z_m alaphalmaz;·)
	asszociatív	asszociatív
	kommutatív	disztributív
	J egységelem	kommutatív (egységgyűrű)
	J inverz	J egységelem(egységgyűrű)

- test

Test	(Z_m alaphalmaz;+)	(Z_m alaphalmaz;·)
	asszociatív	asszociatív
	kommutatív	kommutatív
	J egységelem	J egységelem
	J inverz	J inverz
		disztributív

Feladat

- Z_6=$(0)_6, (1)_6, (2)_6, (3)_6, (4)_6, (5)_6,$
- Z_5=$(0)_5, (1)_5, (2)_5, (3)_5, (4)_5$

Feladat

Test	(Z_6 alaphalmaz;+)	(Z_6 alaphalmaz;·)
	asszociatív	asszociatív
	kommutatív	kommutatív
	J egységelem (0_6)	J egységelem
	J inverz	J inverz
	(0)6 ->(0)6	(1)6 ->(1)6
	(1)6->(5)6	(2)6->nincs
	(2)6 ->(4)6	(3)6->nincs
	(3)6->(3)6	(4)6->nincs
	(4)6->(2)6	(5)6->(5)6
	(5)6->(1)6	

Feladat

Test	(Z_5 alaphalmaz;+)	(Z_5 alaphalmaz;·)
	asszociatív	asszociatív
	kommutatív	kommutatív
	J egységelem (0_5)	J egységelem
	J inverz (0)5 ->(0)5 (1)5->(4)5 (2)5 ->(3)5 (3)5->(2)5 (4)5->(1)5	J inverz (1)5 ->(1)5 (2)5 ->(3)5 (3)5 ->(2)5 (4)5 ->(4)5

Köszönöm a figyelmet!