Eötvös Loránd Tudományegyetem
Természettudományi Kar

Titkosítási módszerek

BSc Szakdolgozat

Készítette: Barsi Réka
Matematika BSc, Matematikai elemző szakirány

Témavezető: Villányi Viktória
Eötvös Loránd Tudományegyetem, Természettudományi Kar
Operációkutatási Tanszék

Budapest, 2020.

NYILATKOZAT

Név: BARSI RÉKA

ELTE Természettudományi Kar, szak: MATEMATIKA BSC

NEPTUN azonosító: X16GYK

Szakdolgozat címe:
TITKOSÍTÁSI MÓDSZEREK

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2020.12.16

a hallgató aláírása

Köszönetnyilvánítás

Szeretnék köszönetet mondani Villányi Viktória témavezetőmnek, a szakdolgozatom írásához adott segítségéért, ötleteiért és jó tanácsaiért.

Köszönöm még a családomnak, páromnak és barátaimnak, akik végig támogattak és biztattak az egyetemi éveim alatt.

Tartalomjegyzék

Bevezetés **6**

1. A kriptográfia **8**

1.1. A kriptográfia áttekintése 8

2. Szimmetrikus kulcsú eljárások **10**

2.1. A spártai szkütalé 10

2.2. Julius Caesar rejtjelezője 11

2.3. A Vigenère-rejtjel 12

2.4. Hill titkosítás 13

3. Aszimmetrikus kulcsú eljárás-RSA **16**

3.1. A megértéshez szükséges tételek, definíciók 16

3.2. RSA algoritmus 18

4. Prímkeresés **22**

4.1. Fermat-prím 22

4.2. Mersenne-prím 22

4.3. Euler-Fermat-prímteszt 23

4.4. Miller-Rabin-prímteszt 23

4.5. Solovay–Strassen prímteszt 24

5. Egész számok faktorizációja **25**

5.1. Próbaosztás 25

5.2. Fermat-féle faktorizáció 26

5.3. Monte-Carlo módszer 27

6. Diffie-Hellman kulcscsere **29**

6.1. Diffie-Hellman kulcscsere támadása 30

7. ElGamal titkosítás **33**

Bevezetés

Azért erre a témára esett a választásom, mert egy olyan tudományággal szerettem volna foglalkozni, ami mára már a mindennapi életünk részévé vált. A kriptográfia a XX. század közepéig csak a katonai és diplomáciai alkalmazásokban jelent meg. A század második felében kezdett megjelenni az üzleti életben is, főként a banki szférában. A XX. század végétől már a mindennapi életet is átszövik az információk tárolásával, továbbításával és feldolgozásával, például:

- interneten történő fizetések biztonsága
- mobiltelefonok biztonsága
- e-mail küldés biztonsága

A témaválasztásomat az is indokolja még, hogy az egyetemen volt egy Digitális aláírások, valamint egy Adatvédelem nevű szabadon választható tárgyam. Az előbbi tárgyat a témavezetőm tartotta és már ekkor eldöntöttem, hogy hasonló témában szeretném írni a dolgozatomat. Inspirált az ezeken az órákon megszerzett tananyag és szerettem volna még több különböző titkosítási módszert megismerni.

A szakdolgozatomban a kriptográfia két fajtájáról a szimmetrikus és az aszimmetrikus kulcsú titkosításokról esik szó.

A dolgozat elején egy rövid kis áttekintést szeretnék nyújtani magáról a titkosításról. Ezután az első részben néhány szimmetrikus rejtjelezőről esik szó, amik közül néhány az időszámításunk elé nyúlik vissza.

A szakdolgozatom második felében részletesebben az aszimmetrikus vagy más néven nyílt kulcsú titkosításokat fogom bemutatni, azon belül is az RSA és az ElGamal módszereket. Néhány prímkereső algoritmusról is szó lesz, amire főként az RSA titkosításnál

lesz szükség.

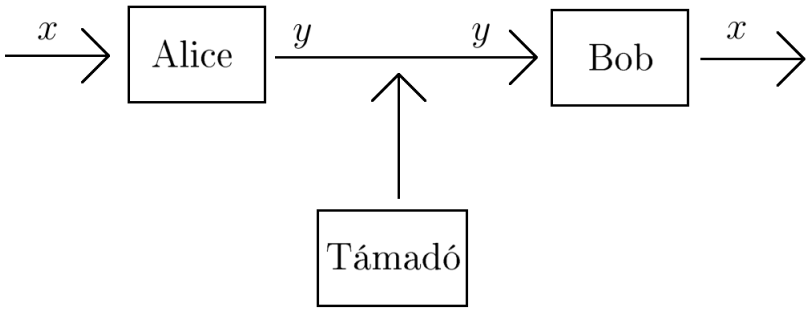
Célom, hogy egy átfogó képet alkossak a különféle módszerekről, valamint remélem, hogy a munkám az olvasók számára érdekes lesz és egy megfelelő összefoglalást kapnak.

1. fejezet

A kriptográfia

1.1. A kriptográfia áttekintése

A kriptográfia egy ógörög eredetű kifejezés, ami a (kryptós) azaz „rejtett”, valamint a (gráphein), „írni” szavak egyesítéséből jött létre. Magyarul legjobban a titkosírás a megfelelő szó rá, de általában maradunk a kriptográfia kifejezésnél. A kriptológia a kommunikáció biztonságossá tételével foglalkozó tudomány, mely két részből áll. A kriptográfia, amely az üzenetek titkosítását és hitelességét biztosító algoritmusokkal, a kriptoanalízis, ami pedig az algoritmusok feltörésével foglalkozik. Ez a két ág együtt biztosítja a megfelelő védelmet.



1.1. ábra. A kommunikáció egy támadó jelenlétében

Az 1.1. ábrán látható a kommunikáció modellje egy támadó jelenlétében, melyen Alice szeretne átküldeni egy üzenetet Bobnak, egy olyan csatornán keresztül, amihez egy har-

madik fél is hozzáfér. Ezért Alice valamilyen módon titkosítja az üzenetet és azt fogja elküldeni Bobnak, aki dekódolja a kapott szöveget és így már ő is tudja értelmezni. A támadó viszont csak a titkos üzenetet tudja megszerezni, így arról nem lesz tudomása, hogy miről is szól az üzenet.

A támadónak két fajtája van: passzív és aktív. A passzív támadó, más néven lehallgató az adatokat szeretné megszerezni. Ezt a támadás típust a titkosítással teljes mértékben meg tudjuk akadályozni. Az aktív támadó viszont nem csak megszerezni próbálja az adatokat, hanem módosítani is, úgy, hogy adatokat von ki, ad hozzá vagy módosít. Sajnos ezt a támadást teljes mértékben nem tudjuk elkerülni.

Sokáig úgy vélték, hogy nem csak a titkosítás kulcsát, hanem magát a titkosítás módszerét is titokban kell tartani. Auguste Kerckhoffs von Nieuwenhof 1883-ban hozta nyilvánosságra elvét, miszerint a titkosítás biztonsága nem függhet attól, hogy ismert-e a titkosítás algoritmusa, csakis a kulcs garantálja a biztonságot. Egy titkosítási rendszer biztonsága a következő lehet:

- elméletileg biztonságos, ha sehogy sem lehet feltörni, azaz akkor sem feltörhető ha a támadónak végtelen számítási eszköz áll a rendelkezésére.
- gyakorlatilag biztonságos, ha a szükséges támadási idő vagy a támadó tárkorlátja lehetetlenné teszi a rendszer feltörését.
- nem biztonságos, ha a feltöréshez elegendő a tár és időkapacitás.

Legtöbbször a célunk az, hogy gyakorlatilag biztonságos titkosítást alkalmazzunk.

Egy üzenetet akkor tekinthetünk titkosítottnak, ha a küldő az üzenetet olyan formátumban küldi el, amit akár többen is el tudnak olvasni, de megérteni csak azok értik meg, akiknek az üzenet küldője szánja. A titkosító algoritmus, amivel a küldő kódolja az üzenetet egy matematikai függvény, amiről fel kell tennünk, hogy injektív. Ez azért fontos, hogy a fogadó egyértelműen vissza tudja fejteni a kódolt üzenetet.

1. Definíció. Az $F\colon A \to B$ függvény injektív (vagy $1-1$ leképezés), ha minden $x_1, x_2 \in A$ esetén igaz, hogy ha $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$.

A későbbiekben megismerkedünk néhány titkosító algoritmussal.

2. fejezet

Szimmetrikus kulcsú eljárások

A XX. századig általában szimmetrikus kulcsú rejtjelezéseket alkalmaztak, azaz az a kulcs amivel az üzenet küldője kódolta az üzenetet, megegyezik a dekódoló kulccsal. Ezért is nevezik még egykulcsos titkosító eljárásnak. Ezeknél az eljárásoknál a közös kulcsot mindkét félnek ismernie kell és titokban kell tartania, hogy nehogy egy harmadik fél is dekódolni tudja az üzenetet.

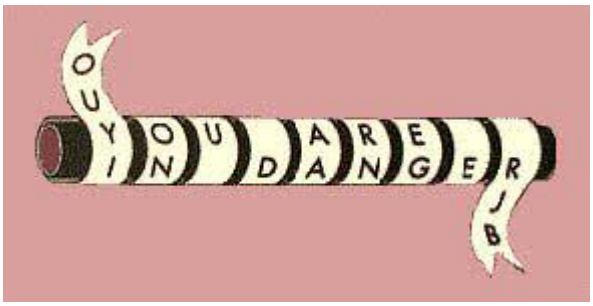
A hétköznapi életben is találkozhatunk a szimmetrikus titkosítással. Például ha banki átutalást hajtunk vére, akkor a számítógépünk és a bank szamítógépe cserél egy csak az általuk ismert szimmetrikus kulcsot.

Valójában már több ezer évvel ezelőtt is használták az ilyen kulcsú titkosításokat. Hadvezérek az utasításaikat titkosítva küldték el, mert tudták, hogy az ellenség mindent megtesz annak érdekében, hogy terveiket előre megtudják, ezért ha, esetleg az üzenet vivőjét útközben elfogják, akkor sem fogják tudni, hogy mire készülnek mert nem tudják elolvasni az üzenetet.

2.1. A spártai szkütalé

A spártai szkütalé egy hatszög alapú hasábból , valamint egy erre tekert pergamenből állt. Az üzenet küldője rátekerte a hasábra a pergament és így írta rá az üzenetet, hosszanti irányba. Ezután letekerték a pergament és így egy értelmetlen szöveget kaptak. A futár derékszíjként viselve vitte el az üzenetet a címzettnek, aki egy ugyanilyen átmérőjú

és ugyanakkora sokszög alapú hasábra tekerve a pergament azonnal értelmezni tudta a kódolt üzenetet. Lüszandrosz, egy spártai hadvezér a szkütalé-nek köszönheti egy perzsa támadás visszaverését, amiről ennek az eszköznek a segítségével értesült.



2.1. ábra. szkütalé

2.2. Julius Caesar rejtjelezője

Julius Caesarról tudjuk, hogy üzeneteit olyan módon kódolta, hogy a betűket az abc-ben valahány hellyel eltolta és az ott lévő betűt írta le. Ha esetleg az abc végére ért, akkor az elejével folytatta. Tegyük fel, hogy minden betűt 10 hellyel tolunk arrébb.

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
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j

2.2. ábra. Helyettesítő táblázat

A táblázat segítségével titkosítsuk az alábbi szöveget: „Szimmetrikus kulcsu eljarasok”. A kódolt üzenet ez lesz: „cjswwodbsuec uevme ovtkbkcyu”. A visszafejtés nagyon egyszerű, nem előrefele hanem visszafele toljuk el a betűket 10 hellyel. Ha a betűk helyett számokat veszünk 0-25-ig, akkor már a számítógép segítségével egyszerűen kiszámolhatunk minden karaktert. Az ötlet az, hogy a kódolt számot úgy kapjuk meg, hogy az eredetihez hozzáadunk 10-et. Ha a kapott szám nagyobb, mint 25, akkor kivonok az eredményből 26-ot, és így megkapjuk a kódolt számot. Modulo segítségével megfogalmazva

először egy példára, az r betűre, aminek a megfelelője a 17.

$$E(17, 10) = 17 + 10 \quad modulo \quad (26)$$

$$E(17, 10) = 1 \quad modulo \quad (26).$$

Tehát az r betű titkosítva a b betű lesz. Általánosan megfogalmazva

$$E(u, k) = u + k \quad modulo \quad (26),$$

ahol $u \in U$, $U = \{0, 1, 2, ...25\}$, k pedig a kulcs, amennyivel eltolom a betűt a titkosítás során.

2.3. A Vigenère-rejtjel

A Vigenère-rejtjel több, különböző Caesar kódok sorozatát használja, attól függően, hogy mit választunk kulcsszónak. Legyen a kulcsszavunk a MATEK. Ekkor a titkosítás, úgy fog kinézni, hogy az első betűt úgy kódolom, hogy az ABC első betűje az m betűnek fog megfelelni, tehát $a = m$. A második betű esetén $a = a$, harmadik esetén $a = t$, negyedik esetén $a = e$, ötödik esetén $a = k$. Majd kezdjük az egészet elölről.

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
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
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
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j

2.3. ábra. Vigenère tábla, MATEK kulcsszóval

A 2.3. ábra segítségével már könnyen titkosíthatunk. Legyen a titkosítandó szöveg a következő: „Kriptografia” . Az első betűt igazából 12 hellyel tolom arrébb, így lesz belőle w. A második betűt 0 hellyel tolom arrébb, tehát az nem változik, és így tovább. A dekódolt üzenet tehát : „wrbtdagkepua”.

Általánosan megfogalmazva, ahol a kulcs betűinek sorszámai legyenek $\{k_1, k_2, k_3, \ldots, k_p, \ldots k_n\}$,

valamint a titkosítandó üzenet betűi $\{u_1, u_2, u_3, \ldots, u_s, \ldots u_m\}$.

$$E(u_1, k_1) = u_1 + k_1 \quad modulo \quad (26)$$
$$E(u_2, k_2) = u_2 + k_2 \quad modulo \quad (26)$$
$$\vdots$$
$$E(u_s, k_n) = u_s + k_n \quad modulo \quad (26)$$
$$E(u_{s+1}, k_1) = u_{s+1} + k_1 \quad modulo \quad (26)$$
$$\vdots$$
$$E(u_m, k_p) = u_m + k_p \quad modulo \quad (26)$$

2.4. Hill titkosítás

A Hill titkosítást Lester Sanders Hill alkotta meg 1929-ben. A módszer első lépése, hogy az ABC betűit számokká írjuk át, ugyanúgy mint a korábbi Caesar titkosításnál, az a betű lesz a 0 a z betű pedig a 25. A titkosítandó üzenetből alkotott számsorozatot n hosszú szakaszokra bontjuk, és ezekből nx1-es oszlopvektorokat alkotunk. A titkosítás kulcsa egy nxn-es mátrix lesz, amit mindegyik oszlopvektorral beszorzok, majd az elemeket modulo (26) veszem és így kapom meg a titkos üzenetet.

1. Példa. *Egy rövid példán keresztül mutatom be a működését. Legyen a titkosítandó üzenet a KRIPTO szó, a kulcs pedig az* $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ *mátrix.*

$$X_1 = \begin{pmatrix} K \\ R \end{pmatrix} = \begin{pmatrix} 10 \\ 17 \end{pmatrix}, \; X_2 = \begin{pmatrix} I \\ P \end{pmatrix} = \begin{pmatrix} 8 \\ 15 \end{pmatrix}, \; X_3 = \begin{pmatrix} T \\ O \end{pmatrix} = \begin{pmatrix} 19 \\ 14 \end{pmatrix}.$$

Számoljuk ki az MX_1, MX_2, *valamint* MX_3 *mátrixokat.*

$$MX_1 = \begin{pmatrix} 44 \\ 98 \end{pmatrix}, \; MX_2 = \begin{pmatrix} 31 \\ 77 \end{pmatrix} \; MX_3 = \begin{pmatrix} 47 \\ 113 \end{pmatrix}.$$

Az így kapott mátrixok elemeit vegyük modulo (26).

$$Y_1 = \begin{pmatrix} 19 \\ 23 \end{pmatrix}, \; Y_2 = \begin{pmatrix} 6 \\ 2 \end{pmatrix}, \; Y_3 = \begin{pmatrix} 22 \\ 13 \end{pmatrix}.$$

Ez alapján a kapott titkosított üzenet a TXGCWN.

A dekódolás az M mátrix inverzének segítségével történik. Az inverz mátrixot megszorzom a kapott kódolt mátrixokkal $M^{-1}Y_i$, és ezek elemeit veszem modulo (26).

Ma is általában a szimmetrikus titkosítást alkalmazzák, mert az a gyorsabb, viszont nincs lehetőség arra, hogy mindenki mindenkivel személyesen találkozzon és egy közös kulcsot beszéljenek meg, ezért a közös kulcs megalkotására szokták használni az aszimmetrikus eljárásokat.

3. fejezet

Aszimmetrikus kulcsú eljárás-RSA

Az aszimmetrikus vagy más néven nyilvános kulcsú rejtjelezés esetén nem csak egy kulcsról beszélünk, hanem egy kulcspárról. Az egyik a nyilvános, amit bárki tudhat, ez általában a kódoló kulcs, a másik pedig a titkos kulcs. Tehát itt nincs szükség arra, hogy a két fél egy közös kulcsot határozzon meg, mint a szimmetrikus eljárásoknál. Itt elegendő, ha az üzenet küldője a vevő nyilvános kulcsával titkosítja a saját titkos kulcsát és ezt küldi el. Ezután a vevő a saját tikos kódjával kódolja a kapott üzenetet és ezt küldi vissza a küldőnek. Fontos meggyőződni arról, hogy biztosan annak a nyilvános kulcsát alkalmazzuk, akinek az üzenetet szánjuk és nem egy harmadik, valószínűleg rossz szándékú félét. Nyilván a két kulcs, a nyilvános és a titkos, matematikailag összefüggnek, viszont a titkos kulcsot nem lehet megfejteni csak a nyilvános kulcs ismeretében.

Az RSA az egyik leggyakrabban használt és legjobban működő nyílt kulcsú titkosítási módszer. Az algoritmus elnevezése a három matematikus nevének kezdőbetűje, akik kifejlesztették a módszert: Ron **R**ivest, Adi **S**hamir, Len **A**dleman.

3.1. A megértéshez szükséges tételek, definíciók

2. Definíció (Az Euler-féle -függvény)**.** Tetszőleges n pozitív egész szám esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az n-hez relatív prímek számát jelöli. Értelemszerűen, ha n egy prímszám, akkor $\varphi(n) = n - 1$.

2. Tétel (Euler-Fermat tétel)**.** *Ha a és n relatív prímek, akkor $a^{\varphi(n)} = 1$ modulo (n).*

3. Tétel (A „kis" Fermat-tétel)**.** *Ha p egy prím szám és a és p egymáshoz viszonyítva relatív prímek, ekkor $a^{p-1} = 1$ modulo (p).*

Ebből a tételből következik a „kis" Fermat-tétel másik alakja. Mivel tudjuk, hogy a és p relatív prímek, ezért p nem osztja a-t. Az előző tétel mindkét oldalát a-val beszorozva kapjuk a következő tételt.

4. Tétel. *Ha p egy prím szám, akkor $a^p = a$ modulo (p).*

Viszont ez a tétel tetszőleges a számra is igaz, nem csak akkor, ha p nem osztja a-t. Ugyanis ha osztja, akkor $a = 0$ *modulo* (p), ezt a^{p-1}-nel szorozva azt kapjuk, hogy $a^p = 0$ *modulo* (p), ezért az is igaz, hogy $a^p = a$ *modulo* (p).

3. Definíció (Legendre-szimbólum)**.** A Legendre-szimbólumot a következőképpen jelöljük és értelmezzük:

$$\left(\frac{a}{b}\right) = \begin{cases} 0, & \text{ha a=0 modulo (p)} \\ 1, & \text{ha a}\neq 0 \textit{ modulo } (p) \text{ és } \exists x \in \mathbb{Z},\ \textit{melyre } a = x^2 \textit{ modulo } (p) \\ -1, & \text{ha a}\neq 0 \textit{ modulo } (p) \text{ és } \nexists x \in \mathbb{Z},\ \textit{melyre } a = x^2 \textit{ modulo } (p) \end{cases}$$

Ha $\left(\frac{a}{b}\right) = 1$, akkor a-t kvadratikus maradéknak hívjuk *modulo* (p).

4. Definíció (Jacobi-szimbólum)**.** Legyen $m > 1$ páratlan szám és $m = p_1 \cdot p_2 \dots p_r$, ahol $p_1 \cdot p_2 \dots p_r$ nem feltétlen különböző pozitív prímek, valamint legyen $(a, m) = 1$. Ekkor a Jakobi-szimbólumot a következőképpen jelöljük és értelmezzük:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_r}\right).$$

Ha m prím, akkor a Jacobi-szimbólum megegyezik a Legendre-szimbólummal.

3.2. RSA algoritmus

Az RSA három algoritmusból áll.

1. A kulcsgenerálás
2. Az üzenet titkosítása
3. Az üzenet visszafejtése

	Alice		**Bob**
1.			$n = p \cdot q$
		$\xleftarrow{(n,e)}$	e
2.	$c = m^e \ modulo \ (n)$	$\xrightarrow{(c)}$	
3.			$d = e^{-1} \ modulo \ (n)$
			$m = c^d \ modulo \ (n)$

1. Választunk két nagy prímet, legyen p és q ($p \neq q$), majd szorozzuk össze őket. Az így kapott szám legyen $n = p \cdot q$. Ezután meghatározzuk $\varphi(n)$ értékét, ami értelemszerűen $(p-1)(q-1)$. Ezután választunk egy olyan e számot, amire igaz, hogy $(e, (p-1)) = 1$, valamint $(e, (q-1)) = 1$, azaz $(e, \varphi(n)) = 1$. Ezután kiszámoljuk e inverzét modulo $(\varphi(n))$, azaz keresni kell egy olyan d számot, amire teljesül, hogy $1 < d < \varphi(n)$, valamint $ed = 1$ modulo $(\varphi(n))$. A kulcsunk nyilvános része az (n, e) számpár, a titkos része a (p, q, d) számhármas.

2. Az üzenet titkosítása során a küldő megkeresi a címzett nyilvános kulcsát, ez lesz n és e. A következő módon titkosítja az m üzenetet:

$$c = m^e \ modulo \ (n).$$

A címzett ezt az üzenetet fogja megkapni és ezt kell dekódolnia.

3. A dekódolt üzenetet a következőképpen kapja meg:

$$m = c^d \ modulo \ (n).$$

Lássuk be, hogy így tényleg az eredeti üzenetet kapom vissza. A következő tétel bizonyításával fogom belátni:

5. Tétel. *Tetszőleges m egész számra igaz, hogy*

$$(m^e)^d = m \ modulo \ (n).$$

Bizonyítás. Mivel tudjuk, hogy $e \cdot d = 1 \ modulo \ \varphi(n)$, ezért az is igaz, hogy $e \cdot d = k \cdot \varphi(n) + 1$, valamely k egész számra. Ebből következik, hogy a tétel bizonyításához a következő állítás belátására van szükségünk.

$$m = m^{k \cdot \varphi(n)+1} \ modulo \ (n)$$

Először egy tetszőleges prímszámra igazoljuk $\varphi(n)$ helyett, ami legyen r.

$$m = m^{k(r-1)+1} \ modulo \ (r)$$

Feltesszük, hogy r prím nem osztója m-nek, ekkor a Fermat-tétel miatt

$$(m^{(r-1)})^k = 1^k = 1 \ modulo \ (r),$$

ha viszont feltesszük, hogy r osztója m-nek, akkor

$$m = m^{k(r-1)+1} = 0 \ modulo \ (r).$$

Tetszőleges r prímre beláttuk, most térjünk vissza a mi esetünkre. Mivel $(p-1)$ és $(q-1)$ is osztja $\varphi(n)$-t, ezért

$$m = m^{k\varphi(n)+1} \ modulo \ (p)$$
$$m = m^{k\varphi(n)+1} \ modulo \ (q).$$

Ebből az következik, hogy p és q is osztja $m^{k\varphi(n)+1} - x$-et, tehát n is osztja. Sikerült belátni, hogy

$$m = m^{k\varphi(n)+1} \ modulo \ (n).$$

□

6. Példa. *Nézzünk egy példát. Legyen* $p = 43$, $q = 13$, $e = 5$, $m = 4$. *Az* n *számot könnyen megkapjuk,* $n = 43 \cdot 13 = 559$. *Ezután kiszámoljuk* $\varphi(n)$ *értékét. Mivel* p *és* q *is prímszám, így* $\varphi = (p-1)(q-1) = 42 \cdot 12 = 504$. *Ezután ellenőrizzük, hogy a választott* e *szám megfelelő-e.* $(5, 504) = 1$, *tehát megfelelő az* e *paraméter. Az* e *inverzét, azaz a* d *számot az Euklédeszi algoritmus segítségével kapom meg.*

$$504 = 5 \cdot 100 + 4$$
$$5 = 4 \cdot 1 + 1$$
$$4 = 1 \cdot 4 + 0,$$

továbbá

$$\begin{aligned} 4 =& 504 - 5 \cdot 100 \\ 1 =& 5 - 1 \cdot 4 = \\ =& 5 - 1 \cdot (504 - 5 \cdot 100) = \\ =& 101 \cdot 5 - 1 \cdot 504, \end{aligned}$$

innen azt kapjuk, hogy

$$101 \cdot 5 = 1 \ \textit{modulo}\ (504),$$

tehát

$$d = 101.$$

Most következik, hogy az $m = 4$ *üzenetet kódoljuk.*

$$c = 4^5 \ \textit{modulo}\ (559)$$
$$c = 465.$$

A dekódolás pedig a következő művelettel történik,

$$m = 465^{101} \ \textit{modulo}\ (559)$$

Először is felbontom a 465^{101} *számot a* 465 *hatványainak szorzatára.*

$$m = \left(\left((465)^4\right)^4\right)^4 \cdot \left(\left((465)^4\right)^4\right)^2 \cdot (465)^4 \cdot (465)^1 \quad \textit{modulo}\ (559)$$

Ezután a zárójeleknél bentről haladva kiszámolom a $(465)^4$ *értékét modulo* (559), $(465)^4 = 484$ *modulo* (559).

$$m = \left((484)^4\right)^4 \cdot \left((484)^4\right)^2 \cdot 484 \cdot 465 \quad \textit{modulo } (559)$$

Ezután a következő hatvány amit kiszámolok, az a $(484)^4$ *modulo* (559), $(484)^4 = 107$ *modulo* (559).

$$m = 107^4 \cdot 107^2 \cdot 484 \cdot 465 \quad \textit{modulo } (559)$$

A legutolsó lépésben két hatványt számolok ki: $(107)^4 = 250$ *modulo* (559) *és* $(107)^2 = 269$ *modulo* (559)

$$\begin{aligned} m &= 250 \cdot 269 \cdot 484 \cdot 465 \quad \textit{modulo } (559) \\ m &= 15135285000 \quad \textit{modulo } (559) \\ m &= 4 \quad \textit{modulo } (559) \end{aligned}$$

Jól látható, hogy a dekódolás után ténylegesen az eredeti üzenetet kaptam vissza.

4. fejezet

Prímkeresés

Az RSA algoritmus megfelelő használatához nagy prímekre van szükségünk, ugyanis ha p-t és q-t túl kicsi prímszámnak veszem, akkor az algoritmus könnyen feltörhető lesz, amit szeretnénk elkerülni. A következő részben pár prímkereső módszert mutatok be, amik alapja, hogy egy nagy számról eldöntsék, hogy nagy valószínűséggel prím vagy összetett szám.

4.1. Fermat-prím

Fermat úgy vélte, hogy $F_n = 2^{2^k} + 1$ alakú számok mindig prímek. Ez az állítás igaz is $n = 1, 2, 3, 4$ esetekre. Euler volt aki bebizonyította, hogy az F_5 nem prím, hanem összetett szám.

A Fermat-számokra alkalmazható egy speciális prímteszt, a Pepin-teszt. F_n pontosan akkor prím, ha

$$3^{\frac{F_n-1}{2}} = 1 \; modulo \; (F_n) \; igaz.$$

4.2. Mersenne-prím

Az $M_p = 2^p - 1$ alakú számokat nevezzük Mersenne-számoknak. Mersenne 1644-ben megjelent könyvében azt írta, hogy $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ értékekre M_p prímszám és minden más 257-nél kisebb számra összetett. Először csak 1876-ban találtak az állításában hibát. Az M_{67} számra bizonyította be Lucas, hogy nem prím. A

későbbiekben még négy hibát találtak, az egyik, hogy az M_{257} összetett szám, valamint, hogy az M_{61}, M_{89}, M_{107} számok is prímek.

A Mersenne-számokra is tudok alkalmazni egy speciális prím-tesztet, a Lucas–Lehmer-tesztet. Legyen p egy páratlan prím, valamint $a_1 = 4$ és $a_{i+1} = {a_i}^2 - 2$, ha $i \geq 1$. M_p pontosan akkor prím, ha $M_p | a_{p-1}$.

4.3. Euler-Fermat-prímteszt

Ennek a prímtesztnek az alapja a korábban említett kis Fermat-tétel. Ha egy n tetszőleges egész számra nem teljesül a tétel, azaz hogy $a^{n-1} = 1$ *modulo* (n), akkor n biztosan összetett szám. Tehát elég egyetlen egy ilyen a számot találni és már tudjuk is, hogy n nem prím. Viszont sajnos ha egyetlen ilyen a számot sem találunk, akkor sem lehetünk biztosak abban, hogy n prím.

5. Definíció (Fermat-tanú)**.** Legyen $n > 1$ tetszőleges egész szám, valamint a egy olyan egész szám, amire nem teljesül a következő kongruencia.

$$a^{n-1} = 1 \; modulo(n)$$

Ekkor a az n összetettségének Fermat-tanúja.

Ha n összetett számhoz nem létezik egy Fermat-tanú sem, akkor a számot Carmichael-számnak nevezzük, a legkisebb ilyen szám az 561.

4.4. Miller-Rabin-prímteszt

Legyen $p > 1$ páratlan egész szám, valamint q egész és r egész, páratlan szám, melyekre igaz, hogy

$$p - 1 = 2^q r.$$

Véletlenszerűen válasszunk egy b bázist. Ha erre a b-re igaz, hogy

$$b^r = 1 \; modulo \; (p),$$

vagy

$$b^{2^k r} = -1 \; modulo \; (p),$$

valamely $0 \leq k < q$ számra, akkor n prímgyanús, ha nem teljesül akkor pedig összetett szám.

Annak a valószínűsége, hogy egy véletlenszerűen választott b mellett, egy összetett szám átmegy a Miller-Rabin-prímteszten, kisebb, mint $\frac{1}{4}$. Értelemszerűen, ha n darab bázist választunk, egymástól függetlenül, akkor annak a valószínűsége, hogy egy összetett szám átmegy a teszten $\left(\frac{1}{4}\right)^n$

7. Példa. *Nézzünk egy példát, amiben legyen $p = 97$. A $p - 1 = 96$ értékét kell felbontanunk, úgy hogy addig osztjuk 2-vel ameddig páratlan számot nem kapunk. A 96-ot ötször tudom elosztani 2-vel és a maradék 3 lesz. Tehát $q = 5$ és $r = 3$. Nézzük, hogy teljesül-e az első állítás, azaz, hogy $b^r = 1$ modulo (p).*

$$2^3 = 8 \ modulo \ (97)$$

Ez az állítás nem igaz, így nézzük meg a másodikat is, ami az, hogy $b^{2^k r} = -1$ modulo(p), valamely $0 \leq k < q$ számra. Először nézzük a $k = 0$ esetet.

$$2^{2^0 \cdot 3} = 8 \ modulo \ (97)$$

$K = 0$-ra nem teljesül az állítás így menjünk tovább.

$$2^{2^0 \cdot 3} = 8 \ modulo \ (97)$$
$$2^{2^1 \cdot 3} = 64 \ modulo \ (97)$$
$$2^{2^2 \cdot 3} = 22 \ modulo \ (97)$$
$$2^{2^3 \cdot 3} = 96 \ modulo \ (97)$$

$K = 3$ esetre sikeres volt a teszt, így 97 nagy valószínűséggel prím.

4.5. Solovay–Strassen prímteszt

Legyen $n \geq 3$ páratlan szám, valamint a következő kongruencia egyenlet:

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \ modulo \ (n)$$

Ha létezik olyan a egész szám, amire nem igaz az egyenlőség, akkor n összetett szám. Ha viszont minden a számra igaz, akkor nagy valószínűséggel n prím.

5. fejezet

Egész számok faktorizációja

A korábban említett RSA algoritmus azon alapszik, hogy az egész számok szorzattá alakítása egy matematikailag nehéz feladatnak számít, azaz nincs hatékony módszer arra, hogy meghatározzuk a faktorokat. Ha ismernénk ilyen algoritmust, akkor az RSA könnyedén feltörhető lenne. A következőkben ilyen algoritmusokra nézünk példát, ahol a számok prímtényezős felbontását szeretnénk meghatározni. Először célszerű egy prímtesztet elvégezni, hogy feleslegesen ne számoljunk túl sokat.

5.1. Próbaosztás

Ez egy egyszerű faktorizációs eljárás, viszont csak kis számokra alkalmazható. Ugyanis nagyon sok időt vesz igénybe. Először nézzük meg egy prímteszt segítségével, hogy a szám prím-e. Ha igen akkor készen is vagyunk, nem tudjuk további prímekre bontani a számot. Ha n nem prím, akkor akkor nézzük az $2, 3, \ldots, \sqrt{n}$ számok közül a prímeket és hogy melyik az, amelyik maradék nélkül osztja az n számot, legyen ez p_1. Ezután az $n_2 = \left(\frac{n}{p_1}\right)$ számra nézzük meg az $2, 3, \ldots, \sqrt{n_2}$ számokat és így megyünk addig ameddig az osztás eredménye 1 nem lesz.

8. Példa. *Nézzünk egy példát, ahol legyen* $n = 570$. *A legkisebb prím ami osztja az* 570-*et, az a* $p_1 = 2$. *Az osztás után az* $n_2 = \frac{n}{p_1} = \frac{570}{2} = 285$ *számmal megyünk tovább. A* 2 *már nem osztja az* n_2 *számot, így a* $p_2 = 3$ *lesz, ezután ugyanezeket hajtjuk végre addig ameddig a hányados értéke* 1 *nem lesz. Az* $n_3 = \frac{285}{3} = 95$, $p_3 = 5$, $n_4 = \frac{95}{5} = 19$, $p_4 = 19$,

$n_5 = \frac{19}{19} = 1$. *Tehát a prímfelbontás a következő:* $570 = 2 \cdot 3 \cdot 5 \cdot 19$

5.2. Fermat-féle faktorizáció

Ebben a részben olyan eseteket nézünk meg, amikor a szorzattá alakítandó n szám felírható két négyzetszám különbségeként.

9. Tétel. *Ha n egy pozitív páratlan egész szám, akkor az $n = a \cdot b$ alakú faktorizáció és $n = t^2 - s^2$ alakban való felírása között létezik kölcsönösen egyértelmű hozzárendelés, ahol $a \geq b > 0$ és s és t nem negatív egészek.* $n = a \cdot b$

Bizonyítás.

1. Először is nézzük az egyik irányt. $\Rightarrow$

$$n = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

2. Ezután a másik irányt, ami következik a következő egyenlőségből. $\Leftarrow$

$$n = t^2 - s^2 = (t+s)(t-s)$$

□

Ha a és b számok egymáshoz közeliek, akkor az azt is jelenti, hogy a számok közel lesznek $\sqrt{n}$, ebből következik, hogy $\frac{a-b}{2}$ kicsi lesz, valamint az előző tétel bizonyításánál beláttuk, hogy $t = \frac{a+b}{2}$ és $s = \frac{a-b}{2}$, így s is kicsi lesz, amiből pedig az következik, hogy t közel lesz $\sqrt{n}$-hez.

A t szám $\sqrt{n}$-hez való közelsége miatt t megtalálásához először a $\lfloor\sqrt{n}\rfloor + 1$-gyel próbálkozunk és közben nézzük, hogy teljesül-e a $t^2 - n = s^2$ egyenlőség. Ha nem teljesül akkor eggyel növelem t értékét és újra vizsgálom az egyenlőséget. Addig megyünk, amíg nem teljesül.

10. Példa. *Nézzünk egy pédát, amiben az $n = 15943$-at szeretnénk faktorizálni.*
A t megtalálásához először a $t = \lfloor\sqrt{15943}\rfloor + 1 = 127$ esetre nézem az egyenlőtlenséget, $127^2 - 15943 = 186$, ahol 186 nem négyzetszám, így t-t eggyel növelem. $128^2 - 15943 = 441 = 21^2$, tehát sikerült felbontanom n-t két négyzetszám különbségére, $t = 128$, $s = 21$, ahonnan könnyedén megkapjuk, hogy $a = 149$, $b = 107$, tehát $15943 = 149 \cdot 107$.

Látható, hogy az algoritmus akkor működik a legjobban, ha a és b közel vannak egymáshoz, tehát az RSA használatakor nem érdemes közeli prímeket választani, ugyanis akkor a Fermat- féle faktorizációval könnyen feltörhető az algoritmus.

5.3. Monte-Carlo módszer

Monte-Carlo módszert, más néven Pollard-féle ρ heurisztikus módszernek is nevezzük, amit 1975-ben John Pollard publikált. Ezt az algoritmust akkor tudjuk alkalmazni prímosztók meghatározására, ha a faktorizálandó egész szám nem prímhatvány, valamint a prímosztók lehetőleg kicsik.

A módszer alapja, hogy a modulo (n) vett maradékok egy idő után elkezdenek ismétlődni, tehát ciklikusak. Először is választanunk kell egy egyszerű egész együtthatós polinomot, ami legyen az $f(x)$.
Ezután generálunk egy x_0 kezdőpontot, majd végrehajtjuk a következő iterációkat:

$$x_1 = f(x_0) \ modulo \ (n)$$
$$x_2 = f(x_1) \ modulo \ (n)$$
$$\vdots$$
$$x_i = f(x_{i-1}) \ modulo \ (n)$$
$$\vdots$$

Ezután az $(|x_i - x_j|, n)$ értékeket vizsgáljuk, ahol $i > j$, azaz olyan x_i-ket keresünk, amik n szerint különböző maradékosztályban vannak, viszont egy p prímosztó szerint ugyanabban. Ha sikerült találnuk ilyen p-t, akkor ez egy prímosztója lesz n-nek.

11. Példa. *Nézzünk egy példát, amiben az* 1343*-at szeretnénk faktorizáni, és ahol* $f(x) = x^2 + 1$*, valamint* $x_0 = 2$*. Egy táblázat segítségével szemléltetem* x_i *értékeit. Látható, hogy az* x_2 *megegyezik az* x_{14}*-gyel, tehát innentől kezdve a maradékok ismétlődni fognak.*

i	x_i	i	x_i
0	2	8	604
1	5	9	864
2	26	10	1132
3	677	11	203
4	367	12	920
5	390	13	311
6	342	14	26
7	124	15	677

Az $x_{11} = 203$ *és* $x_7 = 124$, *valamint* $x_{11} = 45$ *modulo* (79) *és* $x_7 = 45$ *modulo* (79), *így* $(x_{11} - x_7, 1343) = (79, 1343) = 79$, *tehát a* 79 *osztója az* 1343*-nak. Sikerült is felbontanunk az* 1343*-at* $1343 = 79 \cdot 17$.

6. fejezet

Diffie-Hellman kulcscsere

A Diffie-Hellman protokollt Whitfield Diffie és Martin Edward Hellman alkotta meg 1976-ban, ez volt az első kulcscsere algoritmus. Az algoritmus felhasználható nyilvános és magánkulcsok létrehozására.

Alice		**Bob**
$K_{pr,A} \in \{2, 3, \ldots, p-2\}$		
$g \in \{1, 2, 3, \ldots, p-1\}$		
p prím		
$K_{pub,A} = g^{K_{pr,B}}$ *modulo* (p)	$\xrightarrow{(K_{pub,A}, g, p)}$	
	$\xleftarrow{(K_{pub,B})}$	$K_{pub,B} = g^{K_{pr,B}}$ *modulo* (p)
$A = (K_{pub,B})^{K_{pr,A}}$ *modulo* (p)		$B = (K_{pub,A})^{K_{pr,B}}$ *modulo* (p)

A két résztvevő Alice és Bob. Legyen Alice titkos kulcsa $K_{pr,A} \in \{2, 3, \ldots, p-2\}$, valamint p egy nagy prím és g nagy egész szám, úgy hogy $(p, g) = 1$. Ez azért fontos, hogy a visszafejtés nehezebb legyen. Ezek számok segítségével Alice kiszámolja a nyilvános kulcsát, ami legyen

$$K_{pub,A} = g^{K_{pr,A}} \ modulo \ (p).$$

Ezt az üzenetet fogja Alice elküldeni Bob számára, valamint a p és g értékeket. Ezután

Bob a kapott paraméterek segítségével létrehozza a saját nyilvános kulcsát, ami

$$K_{pub,B} = g^{K_{pr,B}} \ modulo \ (p),$$

ahol $K_{pr,B} \in \{2, 3, \ldots, p-2\}$ Bob titkos kulcsa. A létrehozott kulcsot Bob elküldi Alicenak, ezután mindketten kiszámolják a közös kulcsukat, a következőképpen.

$$A = (K_{pub,B})^{K_{pr,A}} \ modulo \ (p)$$
$$B = (K_{pub,A})^{K_{pr,B}} \ modulo \ (p)$$

Könnyen belátható, hogy a két kulcs megegyezik, mert

$$(g^{K_{pr,B}} \ modulo \ (p))^{K_{pr,A}} = g^{K_{pr,B} \cdot K_{pr,A}} \ modulo \ (p) = (g^{K_{pr,A}} \ modulo \ (p))^{K_{pr,B}}$$

Innentől kezdve ezzel a közös kulccsal tudják majd szimmetrikus titkosítással kódolni az üzeneteiket egymás számára.

Nézzünk egy példát. Legyen $g = 3$, $p = 47$, $K_{pr,A} = 8$, valamint $K_{pr,B} = 10$. Először is Alice kiszámolja a saját publikus kulcsát.

$$K_{pub,A} = 3^8 = 28 \ modulo \ (47)$$

Ezután elküldi Bobnak a három paramétert. Bob is kiszámolja a saját nyilvános kulcsát, majd elküldi Alicenak.

$$K_{pub,B} = 3^{10} = 17 \ modulo \ (47)$$

Ezután mindkét fél kiszámolja a közös kulcsot.

$$A = 17^8 = 4 \ modulo \ (47)$$
$$B = 28^{10} = 4 \ modulo \ (47)$$

6.1. Diffie-Hellman kulcscsere támadása

A Diffie-Hellman kulcscsere nem ad teljes biztonságot abban az esetben, ha egy aktív támadó próbálja meg feltörni az algoritmust. Ebben az esetben a támadó nem csak megszerezni tudja az információkat, hanem képes módosítani is az üzeneteket vagy akár

újakat létrehozni, esetleg törölni. Ezt a fajta támadást „man-in-the-middle attack”-nek nevezzük.

Ebben az esetben is legyen Alice és Bob a két résztvevő, valamint az aktív támadó Oscar, aki megpróbálja a kommunikációs csatornát eltéríteni és Alicenak és Bobnak kiadni magát. Ilyenkor mindketten azt hiszik, hogy egymásnak küldik az üzenetet,valamint hogy a másik féltől kapják. Közben mind a ketten Oscarral kommunikálnak.

Először nézzük meg a kétkulcsos láda esetét, majd nézzük meg, hogyan tudja egy aktív támadó feltörni. Alice el szeretne küldeni egy levelet Bobnak, viszont attól fél, hogy esetleg egy postai dolgozó elolvassa az üzenetet, ezért azt találja ki, hogy egy ládába teszi a levelet és tesz a ládára egy feltörhetetlen lakatot. Ezt elküldi Bobnak, aki szintén rátesz egy feltörhetetlen lakatot és így küldi vissza Alicenak. Ezután Alice leveszi a saját lakatját a ládáról és visszaküldi Bobnak. Végül Bob leveszi a saját lakatját és így már hozzáfér a levélhez. A postán dolgozó Oscar megtudja, hogy hogyan szeretné Alice és Bob titokban tartani az üzenetet, így a következőt teszi. Mikor beérkezik a láda a postára, Oscar ráteszi a saját lakatját és Bobként feladja a csomagot Alicenak. Ekkor Alice leveszi a lakatot és visszaküldi, amikor már Oscar könnyedén el tudja olvasni. Ezek után Oscar Alicenak kiadva magát feladja a csomagot Bob számára, természetesen a saját lakatjával védve, amire Bob ráhelyezi a sajátját és visszaküldi. Végezetül Oscar leveszi a saját lakatját és visszaküldi Bobnak. Így Oscar el tudta olvasni úgy a levelet, hogy sem Alice, sem Bob nem szerzett tudomást róla.

A Diffie-Hellman-kulcscsere esetében is hasanló lenne a helyzet egy aktív támadó jelenlétében. Először is az Alice által elküldött $(K_{pub,A}, g, p)$ hármas megszerzése után, Oscar is létehozza a saját publikus kulcsát.

$$K_{pub,O} = g^{K_{pr,O}} \ modulo \ (p).$$

Ezt fogja Oscar visszaküldeni Alicenak úgy mintha Bobtól kapta volna. Emellett Bobnak nem Alice, hanem a saját publikus kulcsát küldi el g és p mellett. A következő lépésben kiszámolják a közös kulcsot, amiről Alice és Bob azt gondolja, hogy az ő közös kulcsuk,

közben mindketten az Oscarral közös kulcsukat számolják ki.

$$A = (K_{pub,O})^{K_{pr,A}} \ modulo \ (p)$$
$$B = (K_{pub,O})^{K_{pr,B}} \ modulo \ (p)$$

Így, ha ezzel a kulccsal titkosítják az üzeneteiket, akkor Oscar az üzenetek megszerzése után könnyedén dekódolni tudja azokat.

7. fejezet

ElGamal titkosítás

Az ElGamal titkosítást Taher Elgamal alkotta meg 1985-ben, aminek alapja a Diffie-Hellman kulcscsere. Ez az algoritmus is három részből áll.

1. A kulcs legenerálása
2. Az üzenet kódolása
3. A kapott üzenet dekódolása

	Alice		**Bob**
1.	$K_{pr,A1} \in \{2, 3, \ldots, p-2\}$		
	$g \in \{1, 2, 3, \ldots, p-2\}$		
	p prím		
	$K_{pub,A1} = g^{K_{pr,A1}}$ *modulo* (p)	$\xrightarrow{(K_{pub,A1}, g, p)}$	
		$\xleftarrow{(K_{pub,B})}$	$K_{pub,B} = g^{K_{pr,B}}$ *modulo* (p)
2.	$K_{pr,A2} \in \{2, 3, \ldots, p-2\}$		
	$m \in \{2, 3, \ldots, p-1\}$		
	$C_1 = K_{pub,A2} = g^{K_{pr,A2}}$ *modulo* (p)		
	$K_{kzs} = K_{pub,B}^{K_{pr,A2}}$ *modulo* (p)		
	$C_2 = m \cdot K_{kzs}$ *modulo* (p)	$\xrightarrow{(C_1, C_2)}$	
3.			$K_{kzs} = K_{pub,A2}^{K_{pr,B}}$ *modulo* (p)
			$m = C_2 \cdot K_{kzs}^{-1}$ *modulo* (p)

1. A Diffie-Hellman protokollhoz hasonlóan itt is legyen Alice és Bob által generált titkos kulcs $K_{pr,A} \in \{2, 3, \ldots, p-2\}$, $K_{pr,B} \in \{2, 3, \ldots, p-2\}$, valamint p egy nagy prím és g nagy egész szám, úgy hogy $(p, g) = 1$.

   Nézzük meg, hogyan is működik az algoritmus lépésről lépésre. Először Alice létrehozza a saját nyilvános kulcsát.

   $$K_{pub,A1} = g^{K_{pr,A1}} \ modulo \ (p)$$

   Ezután Alice elküldi Bobnak a $(K_{pub,A1}, g, p)$ hármast, amely segítségével Bob is létrehozza a saját publikus kulcsát.

   $$K_{pub,B} = g^{K_{pr,B}} \ modulo \ (p)$$

   Az így kapott kulcsot visszaküldi Alicenak. Eddig az algoritmusunk megegyezett a Diffie-Hellman kulcscserével, azonban most az üzenet titkosítása máshogy fog kinézni.

2. Ennél a titkosítási módszernél a titkos üzenet két részből fog állni. Először is Alice az aktuális üzenethez, amit el szeretne küldeni, generál egy új privát kulcsot, ez a $K_{pr,A2}$. Ennek a segítségével kiszámolja az új publikus kulcsot, amit csak ennek az üzenetnek a titkosítására fog felhasználni.

   $$C_1 = K_{pub,A2} = g^{K_{pr,A2}} \ modulo \ (p)$$

   Ezután ennek a segítségével kiszámolja az adott üzenet titkosítására szolgáló közös kulcsot Bobbal.

   $$K_{kzs} = (K_{pub,B})^{K_{pr,A2}} \ modulo \ (p)$$

   Az üzenet második része pedig maga a titkos üzenet, amit a következőképpen számol ki Alice:

   $$C_2 = m \cdot K_{kzs} \ modulo \ (p)$$

   Miután kiszámolta, Alice elküldi Bobnak a C_1, C_2 párost.

3. Bob először is a közös kulcs kiszámolásával kezd.

   $$K_{kzs} = (K_{pub,A2})^{K_{pr,B}} \ modulo \ (p)$$

Ezt követően már tudja a kapott üzenetet dekódolni.

$$m = c \cdot K_{kzs}^{-1} \; modulo \; (p)$$

12. Példa. *Nézzünk erre is egy példát. Legyen* $K_{pr,A1} = 7$, $K_{pr,A2} = 5$, $K_{pr,B} = 12$, $p = 29$, $g = 2$, *valamint a titkosítandó üzenet* $m = 26$.

1. *Első lépésként számítsuk ki Alice nyilvános kulcsát,*

$$K_{pub,A1} = 2^7 \; modulo \; (29)$$
$$K_{pub,A1} = 12$$

majd Bobét.

$$K_{pub,B} = 2^{12} \; modulo \; (29)$$
$$K_{pub,B} = 7$$

2. *Ezután Alice új privát kulcsával számítsuk ki, az adott üzenethez tartozó publikus kulcsot,*

$$C_1 = K_{pub,A2} = 2^5 \; modulo(29)$$
$$C_1 = K_{pub,A2} = 3$$

majd a közös kulcsot.

$$K_{kzs} = (7)^5 \; modulo \; (29)$$
$$K_{kzs} = 16$$

A közös kulcs segítségével titkosítsuk az $m = 26$ *üzenetet.*

$$C_2 = 26 \cdot 16 \; modulo \; (29)$$
$$C_2 = 10$$

$C = 10$ a titkos üzenet, amit Alice elküld Bobnak. Bob első lépése az lesz, hogy a kapott üzenet alapján kiszámolja a közös kulcsot,

$$K_{kzs} = (3)^{12} \ modulo \ (29)$$
$$K_{kzs} = 16$$

majd ennek segítségével visszafejti az üzenetet.

$$m = 10 \cdot 16^{-1} \ modulo \ (29)$$

Először is a 16^{-1} modulo (29) értékét kell kiszámolnunk, amit az Euklédeszi algoritmus segítségével teszek meg.

$$16x = 1 \ modulo \ (29)$$
$$16x + 29y = 1$$

$$29 = 1 \cdot 16 + 13 \ \rightarrow \ 13 = 29 - 1 \cdot 16$$
$$16 = 1 \cdot 13 + 3 \ \rightarrow \ 3 = 16 - 1 \cdot 13$$
$$13 = 4 \cdot 3 + 1 \ \rightarrow \ 1 = 13 - 4 \cdot 3$$

Továbbá

$$1 = 13 - 4 \cdot (16 - 1 \cdot 13) =$$
$$= 5 \cdot 13 - 4 \cdot 16 =$$
$$= 5 \cdot (29 - 1 \cdot 16) - 4 \cdot 16 =$$
$$= 5 \cdot 29 - 9 \cdot 16$$

Tehát megkaptuk, hogy a 16 inverze -9 modulo (29), így már könnyen dekódoljuk az üzenetet.

$$m = 10 \cdot -9 \ modulo \ (29)$$
$$m = 26$$

Azt látjuk, hogy tényleg visszakaptuk a titkosított üzenetet.

Irodalomjegyzék

[1] *Freud Róbert, Gyarmati Edit,* Számelmélet, *Nemzedékek Tudása Tankönyvkiadó Zrt., 2014*

[2] *Buttyán Levente, Vajda István,* Kriptográfia és alkalmazásai, *Typotex Kiadó, Budapest, 2004*

[3] *Liptai Kálmán,* Kriptográfia, *Budapest, 2011*
https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0038_matematika_Liptai_Kalman-Kriptografia/adatok.html

[4] *Simon Singh,* A rejtjelzés és rejtjelfejtés története, *Park Könyvkiadó, 2001 [1999]*

[5] Informatikai biztonság és kriptográfia,
https://arato.inf.unideb.hu/kovacs.zita/Ibiza/Jegyzet_PA_20110508.pdf#page=11&zoom=100,0,148