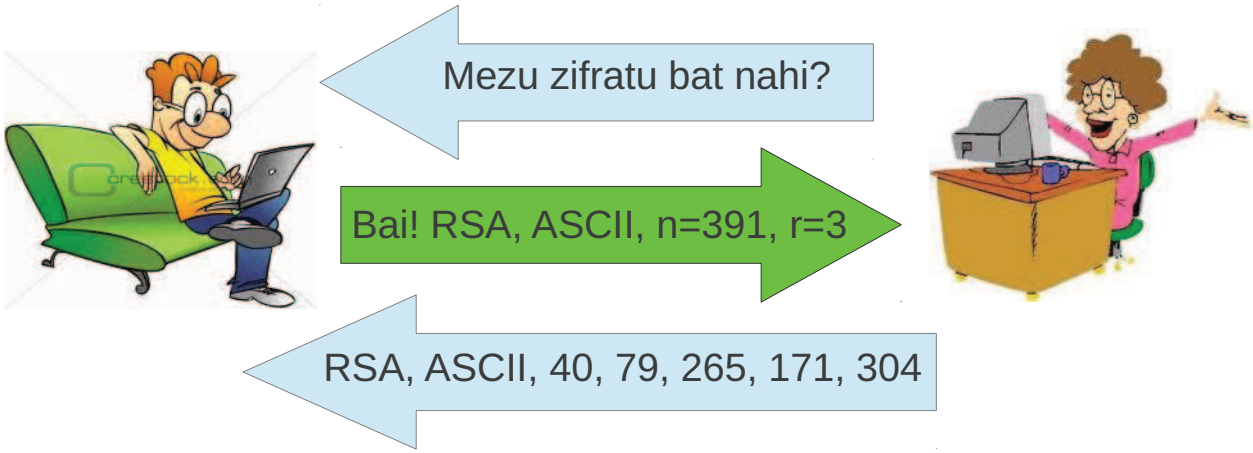
Kriptografia:
RSA zifratze-algoritmoa



Matematika Diskretua
Ana Zelaia Jauregi

Matematika Diskretua
Kriptografia: RSA zifratze-algoritmoa

Kriptografian hain ezaguna den RSA algoritmoa Matematika Diskretua irakasgaian aztertzen dugun Zenbaki Teorian eta Aritmetika Modularrean oinarritzen da. Orri hauetan oinarri matematiko horren azalpen xumea dator, eskola orduetan Zenbaki Teoriari buruz ikasitako kontzeptu matematikoen bidez ulertzeko moduko azalpena, alegia.

1 RSA zifratze-algoritmoa

1977. Urtean Ronald **R**ivest, Adi **S**hamir eta Leonard **A**dleman-ek sortu zuten kriptografia-sistema da RSA. Oso kriptografia-sistema segurua da eta Zenbaki-Teorian eta Aritmetika Modularrean oinarritzen da. Terminologia aldetik esan behar da enkriptatzea eta zifratzea sinonimotzat erabili ohi direla. Mezu zifratua (enkriptatua) mezua jaso behar duenak bakarrik ulertuko du, eta ulertezina gertatzen da gainerakoentzat.

Lagun batek (bidaltzaileak) beste bati (hartzaileari) mezu zifratu bat pasa nahi badio RSA zifratze-sisteman oinarrituz, bai bidaltzaileak eta bai hartzaileak hainbat kalkulu egin beharko dituzte. Honakoak dira, labur-labur esanda, bidaltzaileak eta hartzaileak eman beharko dituzten urratsak:

- Hartzaileak gako publikoa eta pribatua aukeratuko ditu, eta mezu zifratua bidali nahi dion edonori, mezua gako publiko hori erabiliz zifratzeko eskatuko dio. Gako pribatua ezkutuan gordeko du.
- Bidaltzaileak mezu orijinala zenbakitan kodetuko du. Ondoren, gako publikoa erabiliz zifratu egingo du eta mezu zifratua hartzaileari bidaliko dio.
- Hartzaileak gako pribatua erabiliz mezua deszifratu egingo du, eta deskodetu ondoren mezu orijinala, ulergarria dena, lortuko du.

Bidaltzaileak hartzaileari mezua bidali dionean, hau da transmisioaren unean, mezua hartzailea ez den norbaiten eskuetara iristeko arriskua beti existitzen da. Dena den, hala gertatuko balitz ere, berak ez luke mezua ulertuko, mezu zifratua deszifratzeko modu bakarra gako pribatua erabiltzea delako. Gako publikotik abiatuz gako pribatua lor daiteke, eta kalkulatzen saia daiteke, baina konputazionalki ezinezkoa gertatuko zaio.

Hain modu laburrean aipatutako urrats horiek datozen ataletan piskat sakonduko ditugu.

1.1 Gako publikoaren eta pribatuaren aukeraketa

Esan bezala, RSA zifratze-sisteman mezua zifratzeko eta deszifratzeko bi gako erabiltzen dira:

- Gako publikoa: Mezua zifratzeko erabiltzen da. Publikoa da eta edonori eman dakioke.
- Gako pribatua: Mezua deszifratu ahal izateko beharrezkoa den gakoa da. Gako hau pribatua da, mezu hartzaileak sortua eta uneoro ezkutuan gordeko duena.

Gako publikoa eta pribatua kalkulatzeko jarraitu beharreko urratsak honakoak dira:

1. Bi zenbaki lehen p eta q aukeratu, $p \neq q$ (100 digitutik gorakoak).
2. Kalkulatu $n = p \times q$.
3. Gako publikoa (n eta r zenbakiak). $m = \phi(n) = (p-1) \times (q-1)$ izanik, m zenbakiarekin lehen erlatiboa den r zenbaki bat aurkitu behar da, hau da, zkh(m,r)=1 beteko duena. r handia aukeratzea gomendatzen da.
4. Gako pribatua (s zenbakia). r gako publikoaren alderantzizkoa modulu m den s balioa aurkitu behar da, hau da, $s = r^{-1} \bmod m$.

Ikus dezagun adibide bat zenbaki txikiak erabiliz:

1. $p = 17$ eta $q = 23$ zenbaki lehenak aukeratuko ditugu.
2. $n = p \times q = 17 \times 23 = 391 \quad \rightarrow \quad \boxed{n = 391}$.
3. Gako publikoa ($n = 391$, r). r zenbakia aukeratzeko:
   - $m = (p-1) \times (q-1) = (17-1) \times (23-1) = 16 \times 22 = 352 \quad \rightarrow \quad m = 352$.
   - zkh$(m, r) = 1 \quad \rightarrow \quad$ zkh$(352, r) = 1 \quad \rightarrow \quad$ adibidez, $\boxed{\text{r=3}}$.

   r baliorako aukera bat baino gehiago existitzen da. m zenbakiarekin lehen erlatiboa izango den horietako bat aukeratu behar da (txikiena, adibidez).
4. Gako pribatua (s). r-ren alderantzizkoa modulu m den s aurkitu behar dugu, $s = r^{-1} \bmod m$, hau da $rs \bmod m = 1$ beteko duena.
   - $rs \bmod m = 1 \quad \rightarrow \quad 3s \bmod 352 = 1 \quad \rightarrow \quad \boxed{\text{s=235}}$. s balioa Euklidesen algoritmo hedatua erabiliz kalkulatzen da (ikus 2.1. atala).

Hortaz, gako publikoa ($n = 391$, $r = 3$) eta pribatua ($s = 235$) kalkulatuta, RSA zifratze-algoritmoarekin zifratutako mezuak jasotzeko prest dago hartzailea. Egia da gako publikoa den n zenbakia faktorizatuz, p eta q kalkula daitezkeela, eta haiekin m lortu ondoren, gako pribatua den s balioa kalkulatu. Hori dela eta, derrigorrezkoa gertatzen da p, q eta r zenbakiak oso handiak aukeratzea (ikus 2.2. atala).

1.2 Mezua kodetzea/deskodetzea (M_i)

Mezu bat zifratu aurretik kodetu egin behar da, hau da, karakterez osatuta dagoen mezu orijinala zenbakitara bihurtu behar da. Modu berean, zifratuta dagoen mezu bat deszifratu ondoren deskodetu egin beharko da, zenbakietatik abiatuz mezu orijinala osatzen duten karaktereak lortzeko.

Mezuak kodetzeko, kodeketa desberdinak existitzen dira. Kodeketa sinple bat alfabetoko 26 karaktereei 0tik 25erako digituak egokitzea da: $a \leftrightarrow 0$, $b \leftrightarrow 1$, $\cdots$, $z \leftrightarrow 25$. Adibidez, "kaixo"mezuari dagokion mezu kodetua horrela idatziko dugu: 10, 0, 8, 23, 14.

Mezuak kodetzeko beste aukera bat ASCII karaktereen kodeketa erabiltzea da (ikus bibliografia atalean wikipedia erreferentzia). Karaktere inprimagarrien kodeketan kodeketa hamartarrari dagokion zutabea aztertzen baduzu, ikusiko duzu "kaixo"mezua ASCII kodeketa erabiliz horrela geratuko dela: 107, 97, 105, 120, 111.

1.3 Mezua zifratzea/deszifratzea (R_i)

Zifratze-algoritmoak mezuak zifratzeko (enkriptatzeko) erabiltzen dira. Horrela, baimendutako pertsonentzat izan ezik, beste guztientzat mezu zifratua ulertezina gertatzen da.

Nolabait esateko, mezu orijinalari dagozkion kodeak desordenatu egiten dira zifratze-prozesuan. Zifratzeko gako publiko bat erabiltzen da, eta mezua ulertezina bihurtzen da gako pribatua ezagutzen ez duen edonorentzat. Mezu zifratua jaso duen lagunak deszifratze-prozesuaren bidez desordenatuta dauden kodeak ordenatzea lortuko du gako pribatua erabiliz, mezua ulergarri bihurtuko duelarik.

RSA zifratze-algoritmoaren bidez zifratzea zera da: gako publikoa osatzen duten n eta r balioak erabiliz M_i kode bakoitza R_i bihurtzea, aritmetika modularreko honako eragiketaren bidez:

$$\boxed{R_i = M_i^r \bmod n}$$

Deszifratzea, aldiz, gako pribatua den s balioa ezagutzen bada bakarrik burutu daiteke. Horrela, n eta s ezagunak izanik, R_i kode zifratu bakoitza M_i bihurtuko da aritmetika modularreko honako eragiketaren bidez:

$$\boxed{M_i = R_i^s \bmod n}$$

Adibidez, har dezagun "kaixo" mezuari dagokion ASCII kodeketa: $M_1 = 107$, $M_2 = 97$, $M_3 = 105$, $M_4 = 120$, $M_5 = 111$. Mezua ($n = 391$, $r = 3$) gako publikoa erabiliz zifratzeko honako kalkuluak egin behar dira:

- $M_1 = 107 \implies R_1 = 107^3 \bmod 391 = 40.$
- $M_2 = 97 \implies R_2 = 97^3 \bmod 391 = 79.$
- $M_3 = 105 \implies R_3 = 105^3 \bmod 391 = 265.$
- $M_4 = 120 \implies R_4 = 120^3 \bmod 391 = 171.$
- $M_5 = 111 \implies R_5 = 111^3 \bmod 391 = 304.$

Hortaz, mezu zifratua horrela geratuko da: $R_1 = 40$, $R_2 = 79$, $R_3 = 265$, $R_4 = 171$, $R_5 = 304$.

Hartzaileak mezu zifratua deszifratuko du ($s = 235$) gako pribatua erabiliz.

- $R_1 = 40 \implies M_1 = 40^{235} \bmod 391 = 107.$
- $R_2 = 79 \implies M_2 = 79^{235} \bmod 391 = 97.$
- $R_3 = 265 \implies M_3 = 265^{235} \bmod 391 = 105.$
- $R_4 = 171 \implies M_4 = 171^{235} \bmod 391 = 120.$
- $R_5 = 304 \implies M_5 = 304^{235} \bmod 391 = 111.$

Deszifratu ondoren, mezu kodetua lortuko du: $M_1 = 107$, $M_2 = 97$, $M_3 = 105$, $M_4 = 120$, $M_5 = 111$.

2 Zenbaki teoria eta Aritmetika modularra

Esan dugun bezala, RSA zifratze-algoritmoaren oinarri matematikoan Zenbaki Teoria eta Aritmetika Modularra aurkitzen ditugu. Izan ere, gako publikoaren eta pribatuaren kalkuluan zenbaki lehenekin egiten da lan, zatitzaile komunetako handiena kalkulatzen da eta zenbaki baten alderantzizko modularra kalkulatu behar da. Aritmetika modularra mezuak zifratzerakoan eta deszifratzerakoan ere erabili behar da, berreketa modularra kalkulatu behar delako. Zenbaki osoen faktorizazioari buruz ere hitz egin behar da. Atal honetan aipamen berezia egingo diogu alderantzizko modularraren kalkuluari eta zenbaki osoen faktorizazioari. Gainera, frogatuko dugu gako publikoaz zifratutakoa deszifratzea lortuko dela beti gako pribatua erabiliz.

2.1 Alderantzizko modularra

Matematikan, r zenbaki baten alderantzizko zenbakia $\frac{1}{r}$ edo r^{-1} moduan adierazitako beste zenbaki bat da, zeina r balioaz biderkatuz 1 emango duen ($rr^{-1} = 1$). Aritmetika modularrean r zenbaki baten alderantzizkoa modulu m horrela definitzen da: s zenbakia izango da, zeinarentzat $rs \bmod m = 1$ izango den. r zenbaki baten s alderantzizkoa modulu m existitzeko r zenbakiak eta m zenbakiak lehen erlatiboak izan behar dute, hau da, $\text{zkh}(r, m) = 1$ bete behar da. Adibidez, 3 zenbakiaren alderantzizkoa modulu 352 existitzen da, 3 eta 352 zenbaki lehen erlatiboak direlako, zkh(3,352)=1.

Zenbaki baten alderantzizko modularra kalkulatzeko Euklidesen algoritmoa erabili ohi da. Izan ere, frogatuta baitago r eta m bi zenbaki oso emanik, honako konbinazio linealeko s eta v koefizienteak existitzen direla:

$$\forall r, m \in \mathbb{Z} \quad \exists s, v \in \mathbb{Z} \quad \text{non} \quad \text{zkh}(r, m) = sr + vm$$

Frogatuta dago, baita, s koefizientea dela r zenbakiaren alderantzizkoa modulu m. Adibidez, $1 = (-117) \times 3 + (1) \times 352$ betetzen denez, esan dezakegu $s = -117$ dela $r = 3$ zenbakiaren alderantzizkoa modulu 352. Negatiboa denez, aritmetika modularra erabiliz $s = -117 = -117 + 352 = 235$ dela esango dugu. Hortaz, $s = 235$ da $r = 3$ren alderantzizkoa modulu 352. Egiazta daiteke $3 \times 235 \bmod 352 = 1$ betetzen dela.

RSArako gako publikoa eta pribatua kalkulatzen ditugunean, r gako publikotik abiatuz s gako pribatua kalkulatzen dugu $rs \bmod m = 1$ ebatziz. Aritmetika modularraren ikuspegitik horrek esan nahi duena da, bilatzen dugun s gako pribatua r gako publikoaren alderantzizkoa dela modulu m. Gainera, $\text{zkh}(r, m) = 1$ baldintza ezartzen dugu, bilatzen dugun s hori existitzen dela ziurtatzeko.

2.2 Zenbaki osoen faktorizazioa

RSA zifratze-algoritmoan gako publikoa (n eta r balioak) eta gako pribatua (s balioa) matematikoki erlazionaturik daude; n eta r balioak ezagututa, nahikoa izango litzateke n balioaren faktorizazioa kalkulatzea p eta q lortzeko, eta horietatik m kalkulatuz, r balioaren alderantzizkoa kalkulatzea modulu m. Gako publikotik gako pribatua kalkulatzea lortzen bada, RSA enkriptatze-sistemak porrot egin duela esango dugu.

Teorikoki hala da, baina praktikan gako publikoa ezagutu arren, oso zaila gertatzen da gako pribatua kalkulatzea, n balioaren faktorizaziorako ez delako algoritmo eraginkorrik existitzen, n hori oso handia den kasuan. Gaur egun, oso zaila da 200 digitu dituen zenbaki oso bat zenbaki lehenetan faktorizatzea, baina aldi berean 100 digitu dituen zenbaki lehen pare bat aurkitzea eta bi zenbaki horien biderkadura kalkulatzea ez da oso zaila. Hori da RSA enkriptatze-sistemaren arrakastaren oinarria.

2.3 Zergatik funtzionatzen du RSA zifratze-algoritmoak?

Erantzuna berehalakoa da. Eulerren teorema betetzen delako. Ikus dezagun polikiago. Esan dugunez, RSA zifratze-algoritmoaren bidez zifratzea zera da: gako publikoa osatzen duten n eta r balioak erabiliz M_i kode bakoitza R_i bihurtzea, berreketa modularra kalkulatuz:

$$R_i = M_i^r \bmod n$$

Deszifratzea, aldiz, gako pribatua den s balioa ezagutzen bada bakarrik burutu daiteke. Horrela, n eta s ezagunak izanik, R_i kode zifratu bakoitza M_i bihurtuko da horrela:

$$M_i = R_i^s \bmod n$$

Zergatik dakigu berreketa modular horren bidez hasierako M_i lortuko dugula? Hau da, zifratuta zegoena deszifratzea lortuko dugula? Nola froga daiteke hori?

Kontuan izan behar da, n, r eta s zenbakiak ez direla edonola aukeratuak izan. Laburbilduz,

- p eta q bi zenbaki lehen aukeratu eta $n = p \times q$ kalkulatu dugu.
- Ondoren, n zenbakiaren Eulerren funtzioa kalkulatu dugu. Dakigunez, n bi zenbaki lehen desberdinen biderkadura den kasuan $\phi(n) = (p-1)(q-1)$. m notazioaz izendatu dugu Eulerren funtzioa, $m = \phi(n)$.
- r zenbakia aukeratzerakoan $m$rekin lehen erlatiboa den zenbaki bat aukeratu dugu, $\text{zkh}(m, r) = 1$, baldintza horrek bermatzen baitu alderantzizko modularra den $s = r^{-1} \bmod m$ existituko dela (ikus aritmetika modularrean alderantzizko modularraren existentziari buruzko teorema). r eta s elkarren alderantzizkoak direnez, $rs \equiv 1 \bmod m$ betetzen da, hau da, $rs = 1 + k\phi(n)$, $k \in \mathbb{Z}$ izanik.

Hortaz, egin ditzagun kalkuluak. R_i kode zifratua deszifratzeko:

$$R_i^s \bmod n$$

$R_i = M_i^r \bmod n$ berreketa modularraren bidez lortu dugunez,

$$(M_i^r)^s \bmod n \quad \rightarrow \quad M_i^{rs} \bmod n$$

r eta s elkarren alderantzizkoak, $rs \equiv 1 \bmod m \quad \rightarrow \quad rs = 1 + k\phi(n), \quad k \in \mathbb{Z}$

$$M_i^{rs} \bmod n \quad \rightarrow \quad M_i^{1+k\phi(n)} \bmod n \quad \rightarrow \quad M_i M_i^{k\phi(n)} \bmod n \quad \rightarrow \quad M_i (M_i^{\phi(n)})^k \bmod n$$

$\text{zkh}(M_i, n) = 1$ denean, Euler-en teorema aplika dezakegu.

Teorema. (Euler) $a, n \in \mathbb{Z}^+$ lehen erlatiboak izanik, $zkh(a, n) = 1$, $a^{\phi(n)} \equiv 1 \bmod n$.

Ondorioz, $M_i^{\phi(n)} \equiv 1 \bmod n \quad \rightarrow \quad (M_i^{\phi(n)})^k \equiv 1 \bmod n \quad \rightarrow \quad M_i \cdot 1 \bmod n = M_i$

Horrela lortzen da zifratutako R_i kodea deszifratzea, eta M_i berreskuratzea. Oso zaila bada ere, gerta liteke $\text{zkh}(M_i, n) > 1$ izatea. Halakoetan ere Fermat-en teorema txikia erabiliz froga daiteke M_i berreskuratzen dela.

Bibliografia

1. Wikipedian:
   - http://eu.wikipedia.org/wiki/Kriptografia
   - https://eu.wikipedia.org/wiki/Kerckhoffs-en_printzipioak
   - http://eu.wikipedia.org/wiki/Zifratze_algoritmo
   - http://en.wikipedia.org/wiki/RSA
   - https://eu.wikipedia.org/wiki/RSA_faktorizazio-lehia
   - http://eu.wikipedia.org/wiki/ASCII
   - https://eu.wikipedia.org/wiki/Biderketarekiko_alderantzizko_modular
   - https://eu.wikipedia.org/wiki/Zenbaki_osoen_faktorizazio
   - https://eu.wikipedia.org/wiki/Saiakuntzazko_zatiketa
   - https://eu.wikipedia.org/wiki/Alan_Turing
   - https://eu.wikipedia.org/wiki/Joan_Clarke
   - https://eu.wikipedia.org/wiki/Shafrira_Goldwasser
2. Rivest, Shamir, Adleman - The RSA Algorithm Explained

   http://www.youtube.com/watch?v=b57zGAkNKIc
3. "Kode sekretuak (I, II, III)". Patxi Angulo, Elhuyar Zientzia eta Teknika, 78. (1993)
   http://zientzia.eus/artikuluak/kode-sekretuak-i-ii-iii/
4. **Breaking the Code**: Biography of Alan Turing (Derek Jacobi, BBC, 1996)

   http://en.wikipedia.org/wiki/Breaking_the_Code

   http://www.youtube.com/watch?v=S23yie-779k → pelikula

   "Breaking the Code"(1996). A biography of the English mathematician Alan Turing, who was one of the inventors of the digital computer and one of the key figures in the breaking of the Enigma code, used by the Germans to send secret orders to their U-boats in World War II.
5. **The Imitation Game** edo **Descifrando Enigma**:

   The Imitation Game is a 2014 American historical drama thriller film loosely based on the biography Alan Turing: The Enigma by Andrew Hodges (previously adapted as the stage play and BBC drama Breaking the Code). British cryptanalyst Alan Turing, who decrypted German intelligence codes for the British government during World War II.

   https://es.wikipedia.org/wiki/The_Imitation_Game
6. "Kodeen liburua. Simon Singh, Elhuyar Fundazioa, ISBN: 978-84-92457-78-6. Jatorrizko izenburua: "The Code Book".

   http://www.europapress.es/euskera/noticia-elhuyar-fundazioak-simon-singh-idazlearen-the-code-book-liburua-argitaratu-du-euskaraz-20121106134209.html

7. "Enkriptazioa gure inguruko gauza guztietan dago". Elhuyar Zientzia eta Teknika, 291. alea (2012).

   http://aldizkaria.elhuyar.org/elkarrizketak/enkriptazioa-gure-inguruko-gauza-guztietan-dago/

8. "Kriptografia"artikulua Gara egunkarian (2008).

   http://ikusimakusi.net/eu/2008/kriptografia/

9. "Kriptografia: Idazkera Ezkutuaren Artea", Domingo Ramirez-Alzola, Matematika saila, EKAIA (2004), UPV/EHU

   http://www.ehu.es/ojs/index.php/ekaia/article/download/2457/2049

10. "Kriptografia: Komunikazioen Pribatutasuna Babesten". Ana Zelaia Jauregi, GAUR8, naiz.eus (2016)

    https://www.naiz.eus/eu/hemeroteca/gaur8/editions/gaur8_2016-11-19-06-00/pages/30.pdf