DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

13.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Skaitļu teorijas pielietojumi informācijas aizsardzībā

1.1. Vispārēja informācija par šifrēšanu un informācijas aizsardzību

1.1.1. Kriptogrāfijas pamatjēdzieni

Kā aizsargāt datus no nesankcionētas pieejas?

- *fiziskā barjera*- fiziski izolēt informāciju no ienaidniekiem;
- *loģiskā barjera*- uzstādīt sistēmu, kas pārbauda lietotāja pieejas tiesības un kontrolē vai tās tiek pareizi izmantotas;
- *šifrēšana*- uzglabāt un pārsūtīt datus tā, lai ienaidnieki nevarētu tos izmantot, pat ja viņu tiem piekļūst.

Kriptogrāfija (kriptoloģija) - mācība par informācijas slēpšanu, tiek pielietota saistībā ar informācijas drošību (interneta sakari, interneta komercija, militārie sakari u.c.).

Kriptogrāfijas pamatjēdzieni:

- *šifrēšana* - atklātas informācijas (atklātā teksta) pārvēršana nesaprotamā formā (šifrētajā tekstā);
- *dešifrēšana* - operācija, kas ir inversa attiecībā uz šifrēšanu: šifrētā teksta pārvēršana atklātajā tekstā;
- *šifri* - šifrēšanas un dešifrēšanas algoritmi;
- *šifra atslēga* - šifra parametri, kas parasti ir slepeni un tiek bieži mainīti (svarīgos gadījumos tiek izmantoti tikai vienu reizi);

Šifrēšana ir funkcija

$$E : A \times K_E \to S,$$

kur

- A ir atklāto tekstu kopa,
- K_E ir šifrēšanas atslēgu kopa,
- S ir šifrēto tekstu kopa.

Dešifrēšana ir funkcija

$$D : S \times K_D \to A,$$

kur K_D ir dešifrēšanas atslēgu kopa.

Dešifrēšanai bez informācijas par atslēgu (šifra uzlaušanai) ir jābūt ļoti grūtai problēmai, ko nav iespējams atrisināt reālā laikā. Kā noteikt šifra vērtību? Ja šifra uzlaušanas izmaksa ir mazāka kā šifrētās informācijas vērtība, tad šifru var uzskatīt par labu.

Šifrēšanas metode var tikt uzskatīta par drošu, ja izpildās šādi nosacījumi:

- ir pierādīts vai tiek uzskatīts, ka dešifrēšana nav iespējama bez noteiktas matemātiskas problēmas $\mathcal{P}$ atrisināšanas,
- ir pierādīts vai tiek uzskatīts, ka problēmas $\mathcal{P}$ atrisināšana nav iespējama īsā laikā.

Pirms datoru parādīšanās kriptogrāfija nodarbojās galvenokārt ar informācijas slepenības nodrošināšanu militāriem, diplomātiskiem,

ekonomiskiem vai personiskiem mērķiem.

Līdz ar datoru ēras sākumu un ar to saistīto informācijas plūsmas palielināšanos kriptogrāfija nodrošina šādas papildus funkcijas:

- sūtījuma integritātes pārbaude;
- sūtītāja un saņēmēja autentificēšana;
- digitālā paraksta nodrošināšana;
- slepenas informācijas dalīta glabāšana (kādā personu grupā katra persona zina daļu no informācijas, katra k personu grupa var rekonstruēt informāciju, bet grupa, kurā ir mazāk nekā k personu - nevar).

1.1.2. Kriptogrāfijas vēsture

Vēsturiski pirmais aprakstītais šifrēšanas izmantošanas gadījums - Jūlija Cēzara šifri (ap 50BC). Senos laikos lielākā daļa cilvēku neprata lasīt, tāpēc tika izmantoti šādi vienkāršākie šifrēšanas veidi:

- burtu kārtības maiņa vārdos;
- burtu aizvietošana ar citiem burtiem (piemēram, *Cēzara šifrs*, kurā katrs burts tika aizvietots ar to burtu, kas atrodas n pozīcijas tālāk alfabētā, šajā gadījumā atslēga ir skaitlis n).

Ievērosim, ka Cēzara šifrēšana tiek veikta neatkarīgi katram burtam ar formulu

$$E(x) = x + n \pmod{26}$$

un dešifrēšana - ar formulu

$$D(x) = x - n \pmod{26}$$

(burtiem atbilst skaitļi no 0 līdz 26 vai atlikumu klases, burts x tiek aizvietots ar burtu $E(x)$).

Katru sākotnējā teksta burtu x var interpretēt arī kā viendimensionālu vektoru $\overrightarrow{x} = (x)$, un tad Cēzara šifrēšanu var interpretēt arī kā vektoru pārveidojumu

$$E(\overrightarrow{x}) = \overrightarrow{x} + \overrightarrow{n},$$

kur $\overrightarrow{n} = (n)$.

Aizvietošanas šifri ir viegli uzlaužami, ja izmanto statistisko informāciju par burtu biežumu dotajā valodā. Lai atrastu nobīdi, ir jāatrod simbols x, kas šifrētajā tekstā atkārtojas visbiežāk. Ja dotajā valodā visbiezāk atkārtojas burts y, tad nobīde ir vienāda ar soļu skaitu no y līdz x.

Ap 1467.gadu tika izgudrota *polialfabētiskā aizvietošana*, kurā burti tika aizvietoti ar dažādiem burtiem atkarībā no to atrašanās vietas tekstā. Populārākais polialfabētiskās aizvietošanas šifrs - *Vigenère šifrs*, kas darbojas saskaņā ar šādu algoritmu:

- tiek fiksēts atslēgas vārds $K = k_1k_2...k_m$ - parasti vārds vai teikums tajā pašā valodā, kurā tiek rakstīts teksts;

- K tiek savienots pats ar sevi tik ilgi, kamēr savienojums pārsniedz šifrējamā teksta garumu, tiek iegūts vārds $\mathcal{K} = KK...K$;
- $\mathcal{K}$ tiek rakstīts tieši zem šifrējamā teksta;
- šifrējamā teksta burts τ, zem kura atrodas burts κ tiek aizvietots ar to burtu, kas ir nobīdīts no τ par tādu pašu attālumu, par kuru κ ir nobīdīts no burta a.

Ievērosim, ka Vigenère šifrēšana tiek veikta neatkarīgi katram burtam ar formulu

$$E(x_i) = x_i + k_{i \bmod |K|} \pmod{26}$$

un dešifrēšana - ar formulu

$$D(x_i) = x_i - k_{i \bmod |K|} \pmod{26}$$

Vigenère šifrēšana var tikt interpretēta kā vektoru pārveidojums šādā veidā:

- sākotnējais šifrējamais teksts $X = x_1 x_2 ...$ tiek sadalīts virknēs

$$X_1 = (x_1, ..., x_m),$$
$$X_2 = (x_{m+1}, ..., x_{2m}),$$
$$...$$

- katra virkne X_i tiek interpretēta kā m-dimensionāls vektors $\overrightarrow{X}_i$,
- atslēgas vārds K tiek interpretēts kā m-dimensionāls vektors $\overrightarrow{K}$,
- ar katru vektoru $\overrightarrow{X}_i$ tiek veikts šifrēšanas pārveidojums

$$E(\overrightarrow{X}_i) = \overrightarrow{X}_i + \overrightarrow{K}.$$

19.gs vidū tika atklātas metodes Vigenère šifra atšifrēšanai, kas balstījās uz šifrētā teksta aritmētisko progresiju apakšvirkņu (formā $(x_i, x_{i+d}, x_{i+2d}, ...)$) statistisko analīzi - lai uzlauztu šifru, ir jāatrod tāda aritmētiskās progresijas apakšvirkne, kurā simbolu biežuma sadalījums ir tuvs burtu biežuma sadalījumam dotajā valodā.

19.gs beigās kriptogrāfija tika pieņemts *Kerkhofa princips* - lai šifrēšanas metode būtu droša, tai ir jābalstās tikai uz atslēgas slepenību (ir jāpieņem, ka ienaidnieks zina metodi).

Ap 1930.gadu tika izgudrota grūtāk uzlaužama polialfabētiskās šifrēšanas metode - *Hilla metode*, kurā šifrēšana atšķirībā no Vigenère šifrēšanas tiek veikta ar *afīno pārveidojumu*

$$E(\overrightarrow{X}_i) = \mathcal{A}\overrightarrow{X}_i + \overrightarrow{\mathcal{K}},$$

kur $\mathcal{A}$ ir invertējama matrica.

Uz Otrā pasaules kara beigu laiku polialfabētiskā šifrēšana ar elektromehāniskām ierīcēm sasniedza augstu līmeni (piemēram, vācu *Enigma* šifrēšanas mašīna). Šifrēšanas tika veikta ar Vigenere vai Hilla tipa metodēm un garām (šifrējamā teksta garumā) *vienu reizi izmantojamām atslēgām*. Dešifrēšana bija motivējošs faktors elektronisko skaitļošanas ierīču attīstībai. Alans Tjūrings kara laikā bija viens no Britānijas dešifrēšanas darba aktīviem dalībniekiem.

Pēc Otrā pasaulers kara līdz ar datoru attīstību tika izgudrotas sarežģītākas šifrēšanas metodes:

- tiek šifrēti dažāda formāta teksti (piemēram, binārās virknes);
- šifrēšanas tiek veikta simbolu grupām - blokiem;
- tiek intensīvi pielietoti matemātikas (skaitļu teorijas, varbūtību teorijas) sasniegumi.

Datori tika izmantoti arī dešifrēšanā.

Ja abas atslēgas ir slepenas, tādu šifrēšanas metodi sauc par *simetriskās atslēgas* kriptosistēmu. 70.gadu vidū Lielbritānijā (Ellis-Cocks-Williamson) un ASV (Diffie-Hellman) tika izgudrotas vairākas *publiskās atslēgas* kriptosistēmas, kurās viena no divām atslēgām ir zināma visiem, bet otra ir slepena.

80.-90.gados tika izgudrotas vairākas kriptosistēmas, kuru dešifrēšana balstās vienlaicīgi uz vairākām matemātikas sadaļām (veselo

skaitļu teoriju, polinomu teoriju u.c.) Mūsdienās kriptogrāfijas attīstība turpinās.

1.1.3. Simetriskās atslēgas kriptosistēmas

Simetriskās atslēgas kriptosistēma (SAK) ir kriptosistēma, kurā sūtītājam un saņēmējam ir kopīga informācija par atslēgu. Līdz 1976. gadam bija tikai tādas šifrēšanas metodes.

Ir divu veidu simetriskās atslēgas kriptosistēmas:

- plūsmas šifrēšana;
- bloku šifrēšana.

Plūsmas šifrēšana ir līdzīga Vigenere šifrēšanai, kurā atslēga tiek ģenerēta ar slepenu algoritmu palīdzību izmantojot nejaušos skaitļus.

Bloku šifrēšana ir šifrēšanas metode, kurā teksts tiek dalīts apakšvirknēs - blokos (parasti blokā ir 64 vai 128 biti) un katrs bloks tiek šifrēts ar slepenas atslēgas palīdzību.

Kriptogrāfiskā hash-funkcija ir pārveidojums, kas sūtāmo tekstu pārveido par daudz īsāku šifrētu tekstu.

1.1.4. Publiskās atslēgas kriptosistēmas

Publiskās atslēgas jeb *asimetriskā* kriptosistēma (PAK) ir relatīvi jauna metode, kurā viena no šifrēšanas/dešifrēšanas operācijām ir atklāta, bet otra - slepena.

Šī metode tika izstrādāta, lai mazinātu grūtības, kas ir saistītas ar slepeno atslēgu nodošanu visām pusēm, kas piedalās sakaros. Ar šī tipa šifrēšanas metožu palīdzību var vieglāk pārraidīt informāciju pa neaizsargātiem sakaru kanāliem.

Precīzāk, katram lietotājam ir divas atslēgas:

- *publiskā atslēga* (publiski pieejama visiem) un
- *privātā atslēga* (slepena, zināma tikai noteiktam lietotāju lokam).

Abas atslēgas ir saistītas ar noteiktiem matemātiskiem algoritmiem, bet zinot publisko atslēgu, ir praktiski neiespējami atrast privāto atslēgu. Tādējādi, katram lietotājam X ir definētas divas sav-

starpēji inversas funkcijas E_X un $D_X = E_X^{-1}$ tādas, ka

$$E_X \circ D_X = id \text{ un } D_X \circ E_X = id.$$

Funkcija E_X katram X ir publiski zināma.

Šādā kriptosistēmā ir iespējamas divas operācijas:

- (*šifrēšana ar publisko atslēgu*) lai nosūtītu lietotājam X slepenu sūtījumu M, šis sūtījums ir jāaizšifrē ar funkciju E_X, šādā gadījumā tikai X varēs izlasīt sūtījumu $E_X(M)$, pielietojot tam savu slepeno funkciju D_X:

$$D_X(E_X(M)) = M.$$

- (*digitālā paraksta nodrošināšana*) lai lietotājs X varētu pierādīt savu identitāti, viņš/viņa aizšifrē kādu noteiktu tekstu N (piemēram, savu vārdu) ar savu slepeno funkciju D_X, jebkurš sūtījuma $D_X(N)$ saņēmējs var pielietot šim sūtījumam publisko funkciju E_X, izlasīt rezultātu $E_X(D_X(N) = N$ un pārliecināties, ka sūtītājs ir bijis X (vai vismaz kāds, kas zina X slepeno atslēgu).

1.1. piezīme. Viena no lielākajām PAK problēmām - rūpēties par to, ka ienaidnieki nerada kļūdas publiskajās atslēgās. PAK ir darbietilpīgākas no skaitļošanas viedokļa salīdzinājumā ar SAK.

1.2. piezīme. PAK var tikt lietota kombinācijā ar SAK. Piemēram, sūtītājs aizšifrē sūtījumu M ar slepenu šifrēšanas funkciju A, aizšifrē A ar saņēmēja X publisko atslēgu, un nosūta X pāri $(E_X(A), A(M))$.

1.1.5. Steganogrāfija

Steganogrāfija ir mācība par slepenās informācijas slēpšanu kādā aptverošā informācijas vidē, tā lai ienaidnieks nebūtu informēts par slepenās informācijas esamību.

Senos laikos pielietotas steganogrāfijas metodes piemērs - vergam noskuva galvu, uztetovēja sūtījumu un, kad mati atauga, nosūtīja vergu saņēmējam. Viduslaikos tika izgudrotas neredzamās tintes.

Steganogrāfisks sūtījums parasti izskatās kā nevainīgs informācijas kopums - attēls, raksts avīzē, mūzikas gabals.

Steganogrāfija tiek bieži izmantota mūsdienu datortehnoloģijās:

- teksta parametru (pieturzīmju, fontu) izmantošana;
- neredzamo fontu izmantošana;
- interneta sūtījumu aiztures laika variēšana;
- informācijas iekodēšana trokšņa veidā mūzikas failos;

1.2. Publisko atslēgu kriptosistēmu konkrētas realizācijas

PAK balstās uz matemātiķiem zināmu novērojumu, ka ir funkcijas/algoritmi, kuriem ir grūti atrast inversās funkcijas/algoritmus.

Piemēri:

- reizināt ir vieglāk nekā dalīt;
- kāpināt kvadrātā ir vieglāk nekā atrast kvadrātsakni;
- reizināt pirmskaitļus ir vieglāk nekā atrast skaitļa sadalījumu pirmskaitļu reizinājumā;
- atrast $a^b \pmod m$ ir vieglāk nekā atrast $\mathsf{ind}_a(b)$;
- izjaukt puzli ir vieglāk nekā salikt;
- nolobīt olu ir vieglāk nekā salikt atpakaļ čaumalu.

PAKā vieglā funkcija tiek izmantota kā publiski pieejamā funkcija, grūtā (inversā) funkcija tiek izmantota kā slepenā privātā funkcija.

1.2.1. Rivest-Shamir-Adleman (RSA) kriptosistēma

RSA kriptosistēmas atslēgu ģenerēšanas algoritms:

1. Izvēlēties divus lielus pirmskaitļus p un q.
2. Atrast $n = pq$, n tiek lietots kā palīginformācija (modulis) abās atslēgās.
3. Atrast $\varphi(n) = (p-1)(q-1)$.
4. Atrast invertējamu elementu $e \in U_{\varphi(n)}$ tādu, ka $1 < e < \varphi(n)$ $(LKD(e, \varphi(n)) = 1)$, e ir publiskā atslēga.
5. Atrast $d \equiv e^{-1} \pmod{\varphi(n)}$, piemēram, izmantojot Eiklīda algoritmu, d ir privātā (slepenā) atslēga.

Publiski pieejamā informācija - n un e. Slepenā informācija - p, q, d.

RSA šifrēšanas algoritms (funkcija E_X):

1. Sadalīt sūtāmo tekstu M daļās $m_1 m_2 ... m_k$ tā, lai katra daļa m_i būtu mazāka kā n saskaņā ar publiski zināmu algoritmu.
2. Katru teksta daļu m_i pārveidot par $c_i = m_i^e \pmod{n}$. Šifrēšanas rezultāts ir virkne $c_1 c_2 ... c_k$.

Ievērosim, ka inversā funkcija ir saistīta ar e-tās kārtas saknes aprēķināšanu mod n.

RSA dešifrēšanas algoritms (funkcija D_X):

1. Katram i atrast $m_i = c_i^d \pmod{n}$.
2. Savienot atšifrētās daļas m_i vienā virknē.

1.1. teorēma. (*RSA dešifrēšanas algoritma pamatojums*) Ja

$$c \equiv m^e \pmod{\text{n}},$$

tad

$$m \equiv c^d \pmod{\text{n}}.$$

PIERĀDĪJUMS Tā kā $ed \equiv 1 \pmod{\varphi(n)}$, tad

$$ed = 1 + l\varphi(n) = 1 + l(p-1)(q-1)$$

un

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+l\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^l \pmod{\text{n}}.$$

Ja $m \in U_n$, tad saskaņā ar Eilera teorēmu $m^{\varphi(n)} \equiv 1 \pmod{\text{n}}$ un tātad $c^d \equiv m \pmod{\text{n}}$.

Ja $m \notin U_n$, tad vai nu $m \equiv 0 \pmod{\text{p}}$, vai arī $m \equiv 0 \pmod{\text{q}}$. Apskatīsim tikai pirmo gadījumu. Ja $m \equiv 0 \pmod{\text{p}}$, tad

$$m^{ed} \equiv 0 \equiv m \pmod{\text{p}}$$

un

$$m^{ed} \equiv m^{1+l(p-1)(q-1)} \equiv m \cdot (m^{q-1})^{p-1} \equiv m \pmod{q}.$$

Attiecībā uz m^{ed} esam ieguvuši sistēmu

$$\begin{cases} m^{ed} \equiv m \pmod{p} \\ m^{ed} \equiv m \pmod{q}. \end{cases}$$

Saskaņā ar ķīniešu atlikumu teorēmu iegūstam, ka $m^{ed} \equiv m \pmod{pq}$. Esam pierādījuši, ka arī gadījumā, kad $m \equiv 0 \pmod{p}$, izpildās vienādība $c^d \equiv m \pmod{n}$. Līdzīgi tiek pierādīts gadījums, kad $m \equiv 0 \pmod{q}$. ■

1.1. piemērs. Atradīsim RSA kriptosistēmas atslēgas un algoritmus, ja $p = 17$ un $q = 19$:

1. Ir izvēlēti divi pirmskaitļi $p = 17$ un $q = 19$.
2. Atrast $n = pq = 323$, n tiek lietots kā palīginformācija (modulis) abās atslēgās.
3. Atrast $\varphi(n) = (p-1)(q-1) = 288$.
4. Atrast invertējamu elementu $e \in U_{288}$ tādu, ka $1 < e < 288$ $(LKD(e, 288) = 1)$: izvēlēsimies $e = 5$, e ir publiskā atslēga.
5. Atrast $d \equiv e^{-1} \pmod{\varphi(n)}$: $d \equiv 173 \pmod{288}$, d ir privātā (slepenā) atslēga.

Šifrējošā funkcija ir $E(m) \equiv m^5 \pmod{323}$, dešifrējošā funkcija $D(c) \equiv c^{173} \pmod{323}$. Ja $m = 300$, tad

$$E(300) \equiv 300^5 \equiv 78 \pmod{323}$$

un

$$D(E(300)) = D(78) \equiv 78^{173} \equiv 300 \pmod{323}.$$

Atradīsim RSA kriptosistēmas atslēgas un algoritmus, ja $p = 911$ un $q = 919$:

1. Izvēlēties divus pirmskaitļus $p = 911$ un $q = 919$.
2. Atrast $n = pq = 837209$, n tiek lietots kā palīginformācija (modulis) abās atslēgās.
3. Atrast $\varphi(n) = (p-1)(q-1) = 835380$.
4. Atrast invertējamu elementu $e \in U_{288}$ tādu, ka $1 < e < 835380$ ($LKD(e, 835380) = 1$): izvēlēsimies $e = 11$, e ir publiskā atslēga.
5. Atrast $d \equiv e^{-1} \pmod{\varphi(n)}$: $d \equiv 227831 \pmod{835380}$, d ir privātā (slepenā) atslēga.

Šifrējošā funkcija ir $E(m) \equiv m^{11} \pmod{837209}$, dešifrējošā funkcija $D(c) \equiv c^{227831} \pmod{837209}$. Ja $m = 830000$, tad

$$E(830000) \equiv 830000^{11} \equiv 456579 \pmod{837209}$$

un

$$D(E(830000)) = D(456579) \equiv 154392^{227831} \equiv 300 \pmod{837209}.$$

1.2.2. El Gamala kriptosistēma

El Gamala kriptosistēmas atslēgu ģenerēšanas algoritms:

1. Izvēlēties lielu pirmskaitli p un grupas U_p ģeneratoru (primitīvo sakni) g.
2. Izvēlēties nejaušu skaitli a, $1 < a < p-1$ (slepeno atslēgu) un aprēķināt $t = g^a \pmod{\text{p}}$.

Publiski pieejamā informācija - p, g un t. Slepenā informācija - a. Ievērosim, ka slepeno informāciju a var uzzināt, ja atrod $\mathsf{ind}_g(t)$.

El Gamala šifrēšanas algoritms (funkcija E_X):

1. Sadalīt sūtāmo tekstu M daļās $m_1 m_2 ... m_k$ tā, lai katra daļa m_i būtu mazāka kā p saskaņā ar publiski zināmu algoritmu.
2. Izvēlēties skaitli k, $1 \leq k < p - 1$.
3. Katrai teksta daļu m_i pārveidot par $c_i = m_i \cdot t^k \pmod{p}$. Šifrēšanas rezultāts ir pāris $(g^k, c_1 c_2 ... c_k)$.

El Gamala dešifrēšanas algoritms (funkcija D_X):

1. Atrast $t^k = (g^k)^a$.
2. Atrast t^{-k}.
3. Atrast $m_i = c_i t^{-k}$
4. Savienot atšifrētās daļas m_i vienā virknē.

1.2. piemērs. Aprakstīsim El Gamala sistēmu, ja $p = 19$. Atslēgu ģenerēšanas algoritms:

1. $p = 19$ un primitīvā sakne ir $g = 2$.
2. Izvēlamies nejaušu skaitli a, $1 < a < 18$ (slepeno atslēgu), $a = 7$ un aprēķinām $t = 2^7 \equiv 14 \pmod{19}$.

Publiski pieejamā informācija - $p = 19$, $g = 2$ un $t = 14$. Slepenā informācija - $a = 7$.

Šifrēšanas algoritms (funkcija E_X):

1. Šifrēsim tekstu $(11, 12, 13)$.
2. Izvēlēties skaitli k, $1 \leq k < 18$, $k = 3$.
3. Katrai teksta daļu m_i pārveidot par

$$c_i = m_i \cdot 14^3 \equiv m_i \cdot 8 \pmod{\text{p}}.$$

Šifrēšanas rezultāts ir pāris $(g^k, c_1 c_2 ... c_k) = (8, (12, 1, 9))$.

Dešifrēšanas algoritms (funkcija D_X):

1. Atrast $t^k = (g^k)^a = 8^7 \equiv 8 \pmod{19}$.
2. Atrast $t^{-k} \equiv 12 \pmod{19}$.
3. Atrast $m_i = c_i t^{-k}$: $m_1 = 12 \cdot 12 = 11$, $m_2 = 1 \cdot 12 = 12$, $m_3 = 9 \cdot 12 = 13$.
4. Savienot atšifrētās daļas m_i vienā virknē.

1.2.3. Diffie-Hellman atslēgu apmaiņas algoritms

Vēsturiski pirmais algoritms, kurā tika izmantota funkcija ar grūti aprēķināmu inverso funkciju, bija *Diffie-Hellmana atslēgu apmaiņas algoritms*.

Ar šo algoritmu divi subjekti, kas vēlas apmainīties ar slepenu informāciju, var publiski (pa neaizsargātu sakaru kanālu) nodot viens otram informāciju, ar kuras palīdzību var aprēķināt tikai šiem diviem subjektiem zināmu slepenu atslēgu vai informāciju.

Diffie-Hellmana atslēgu apmaiņas algoritms:

1. X un Y izvēlas pirmskaitli p un primitīvo sakni g (mod p).
2. X izvēlas savu slepeno atslēgu $n < p$, Y izvēlas savu slepeno atslēgu $m < p$.
3. X aprēķina g^n (mod p) un sūta to Y kā savu publisko atslēgu.
4. Y aprēķina g^m (mod p) un sūta to X kā savu publisko atslēgu.
5. X un Y aprēķina kopīgo slepeno atslēgu

$$s = g^{nm} \equiv (g^n)^m \equiv (g^m)^n \text{ (mod p)}.$$

Izmantojot s kā šifrēšanas atslēgu, X un Y var sūtīt viens otram slepenus ziņojumus. Lai trešais subjekts atrastu s, viņam/viņai ir jāatrod $\mathsf{ind}_g(g^n)$ vai $\mathsf{ind}_g(g^m)$, kas ir grūti.

1.3. piemērs. Izvēlēsimies $p = 19$, $g = 2$, $n = 6$, $m = 10$. Tad $2^n \equiv 7$ (mod p), $2^m \equiv 17$ (mod p) un $s \equiv (2^n)^m \equiv (2^m)^n \equiv 7$ (mod p).

2. 13.mājasdarbs

13.1 Izmantojot Cēzara šifru ar nobīdi 11 aizšifrējiet tekstu "ienaidnieks mūs ir ielencis" izmantojot latviešu alfabēta standarta kārtību.

13.2 Izmantojot Vigenere šifru ar atslēgas vārdu "livonija" atšifrējiet tekstu "iģtohi" izmantojot latviešu alfabēta standarta kārtību.

13.3 Atrodiet atslēgas un aprakstiet šifrēšanas/dešifrēšanas algoritmus RSA sistēmā ar pirmskaitļiem 11 un 13.

13.4 Atrodiet atslēgas un aprakstiet šifrēšanas/dešifrēšanas algoritmus El Gamala sistēmā ar pirmskaitli 23.