Jelgavas Tehnikums

Kaspars Ļubinskis
Džesija Vilkāja

Metodiskā izstrādne

Kombinatorika kritpēšanas metodoloģijā

Jelgava

2019

Anotācija

Metodiskā materiāla mērķis ir 11.klases izglītjamajiem veidot priekštatu par datorkompletkēšanas un montāžas priekšmeta tēmu kriptogrāfija ar starppriekšmetu saikni matemātikā par tēmu kombinatorika. Uzdevums ir parādīt matemātikas nozīmi paroles sastādīšanas metadaloģijā.

Saturs

1.Stundas tēma, mērķis, uzdevumi un izmantotās metodes

1.1Stundas tēma: Kriptogrāfija 2 nodarbības

Mērķis: veidot priekšstatu par kriptogrāfiju un tās nozīmi IT tirgū.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Ievads teorijā	Pedagogs uzsāk diskusiju par to, kas ir kriptogrāfija	15min
Uzdevums	Kad izglītojamie nonāk līdz atziņai, ka ir savā dzīvē saskārušies ar kriptogrāfiju ,pašiem to nezinot, tad jāizpēta tā. /pētnieciskais darbs.	20min
Secinājumi	Pedagogs ar izglītojamiem izanalizē uzdoto uzdevumu. /situāciju analīze un jautājumi, atbildes	10min
Teorētiskā daļa	Iepazīstināt izglītojamos ar kriptogrāfijas veidiem /stāstījums	15min
Pieredzes apmaiņa	Pedagogs dalās pieredzē, stāstot dzīves piemērus. /stāstījums	10min
Jautājumi	Pedagogs uzdod jautājums par tikko stāstīto tēmu. /jautājumi, atbildes atgriezeniskā saite.	5min
		Kopā:80 min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību materiāli

1.2Stundas tēma: Šifru veidi

Mērķis: veidot priekšstatu par kā darbojas kriptorgrāfijas šifri.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Ievads teorijā	Pedagogs uzsāk diskusiju par to, kas ir šifrs / diskusija	10min
Uzdevums	Kad izglītojamie sapratuši jēdzienu kriptēšana, iepazīstas ar dažādiem šifrēšanas veidiem ./ pētnieciskais darbs.	15min
Uzdevums	Praktiskais darbs izveidot savu šifru, balstoties uz kādu no šifrēšanas veidiem . / darbs grupās	5min
Jautājumi	Pedagogs uzdod jautājums par tikko stāstīto tēmu. / jautājumi, atbildes atgriezeniskā saite.	5min
		Kopā:40min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību materiāli

1.3Tiešo metožu vājums un rotora mašīnas

Mērķis: veidot priekšstatu par kā darbojas kriptogrāfijas šifri.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Ievads teorijā	Pedagogs uzsāk diskusiju par to, kādas ir tiešo metožu trūkums kriptogrāfijas nozarē / diskusija	10min
Uzdevums	Izanalizē savas izstrādātās kritpogrāfijas metodes priekšrocības un trūkumus ./ pētnieciskais darbs.	15min
Teorija	Rotora mašīnas . / stāstījums	5min
Jautājumi	Pedagogs uzdod jautājums par tikko stāstīto tēmu. / jautājumi, atbildes atgriezeniskā saite.	5min
		Kopā:40min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību materiāli

1.4Stundas tēma: Droša šifra metodes 2nodarbības

Mērķis: pārvaldīt izrpast dorša šifra metodes.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Jautājumi atkārtošanai	Pedagogs uzsāk diskusiju par to, kas ir priekšnosacījumi darbam ar kriptogrāfiju. / jautājumi atbildes	15min
Demonstrācija1	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums1	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	15min
Demonstrācija2	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums2	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	15min
Demonstrācija3	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums3	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	10min
Noslēgums	Skolotājs pārliecinās, ka izglītojamie ir tikuši galā ar uzdevumu, uzdevumu pildīšanas brīdī sniedz norādes, kādi ir galvenie akcenti, pildot konkrētās darbības. Darbs tiek vērtēts ar atzīmi / Situāciju izpēte	5min
		Kopā:80min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību materiāli

1.5Stundas tēma: Drošas kritēšanas metodes 2 nodarbības

Mērķis: veidot priekšstatu par kriptogrāfiju un tās nozīmi IT tirgū.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Ievads teorijā	Pedagogs uzsāk diskusiju par to, kādas ir drošas kritēšanas metodes mūsdienās /stāstījums	15min
Uzdevums	Izglītojamie izanalizē, kādi ir galvenie nosacījumi kritpēšanai, lai tā būtu droša /pētnieciskais darbs.	20min
Secinājumi	Pedagogs ar izglītojamiem izrunā uzdoto uzdevumu. /situāciju analīze un jautājumi, atbildes	10min
Teorētiskā daļa	Iepazīstina izglītojamos ar kriptogrāfijas metodēm /stāstījums	15min
Pieredzes apmaiņa	Pedagogs dalās pieredzē, stāstot dzīves piemērus. /stāstījums	10min
Jautājumi	Pedagogs uzdod jautājums par tikko stāstīto tēmu. /jautājumi, atbildes atgriezeniskā saite.	5min
		Kopā:80 min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību materiāli

1.6Stundas tēma: Praktisko darbu izspilde par RSA kritēšanas metodi 2nodarbības

Mērķis: apgūt RSA metodaloģiju.

Stundas struktūra	Pedagoga rīcība/ pielietotā metode	Laiks
Ievads	Iepazīstina izglītojamos ar stundā veicamajiem darbiem. Izstāstot stundas plānu. /stāstījums	5min
Jautājumi atkārtošanai	Pedagogs uzsāk diskusiju par to, kas ir priekšnosacījumi darbam ar kritpogrāfiju. / jautājumi atbildes	15min
Demonstrācija1	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums1	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	15min
Demonstrācija2	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums2	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	15min
Demonstrācija3	Pedagogs nodemonstrē piemērus komandrindu izmantošanai. / demonstrēšana	5min
Uzdevums3	Pedagogs iedod uzvedumu atbilstoši nodemonstrētajam piemēram. / laboratorijas darbs, problēmu risināšana.	10min
Noslēgums	Skolotājs pārliecinās, ka izglītojamie ir tikuši galā ar uzdevumu, uzdevumu pildīšanas brīdī sniedz norādes, kādi ir galvenie akcenti, pildot konkrētās darbības. Darbs tiek vērtēts ar atzīmi / Situāciju izpēte	5min
		Kopā:80min

Tehniskais nodrošinājums: projektors; dators un pedagoga sagatavoti mācību

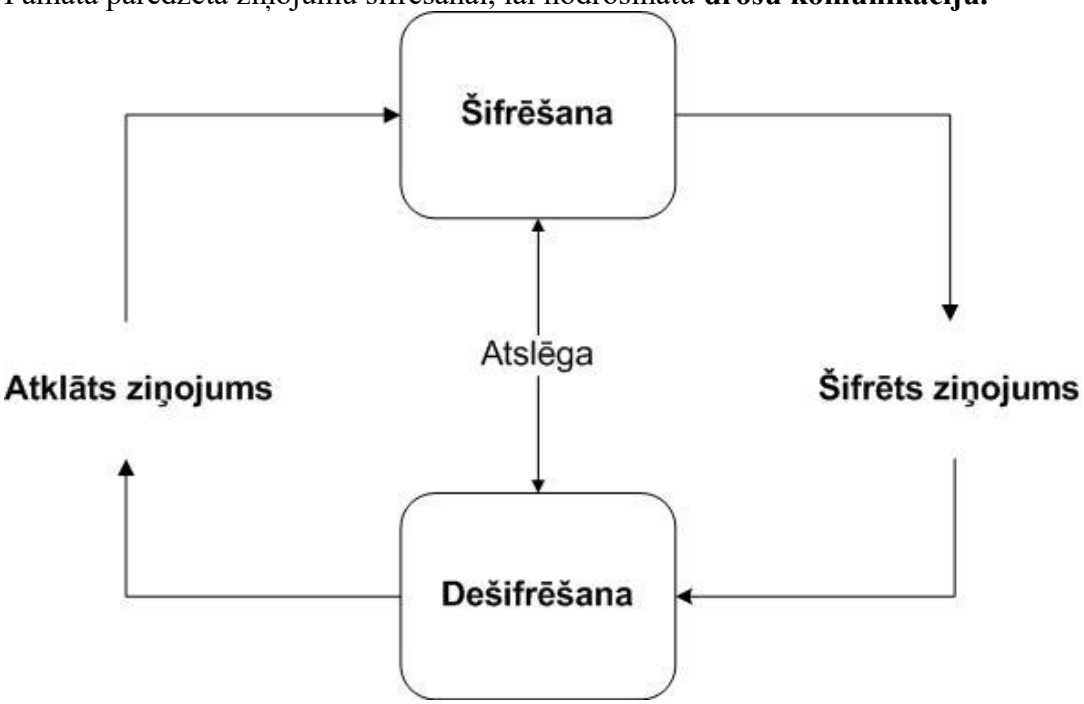
Kriptogrāfija

Kriptogrāfija: Zinātne par ziņojumu kodēšanas metodēm
Tā nodrošina:

- Datu slepenību
- Datu integritāti
- Datu autentifikāciju
- Datu neviltojamību un nenoliedzamību

Integrēta lielākajā daļā aizsardzības mehānismu

Kriptogrāfijas pamata būtība
Pamatā paredzēta ziņojumu šifrēšanai, lai nodrošinātu **drošu komunikāciju.**

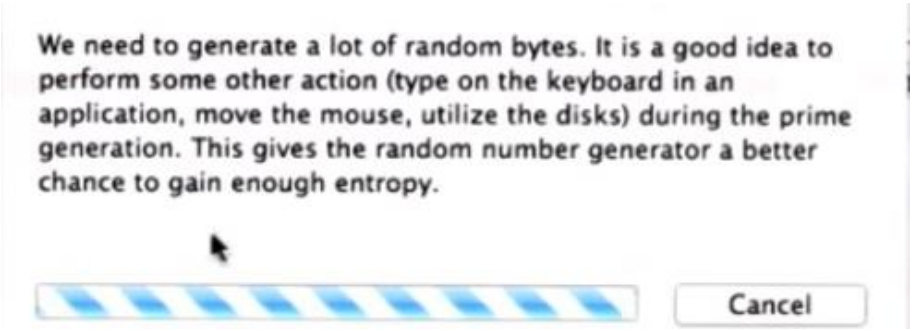


Kriptosistēmas elementi:

- P - pamattekstu kopa;
- C - kriptotekstu kopa;
- K - atslēgu kopa;
- $E: P \times K \rightarrow C$ – šifrs;
- $D: C \times K \rightarrow P$ – dešifrētais teksts;

Pamatā divi soļi – vienojamies par atslēgu un tad komunicējam
Ko nozīmē pilnīgi nejauši (*RANDOM*)
Jānis Banis nodefinēja, ka nejaušība ir**:**
K(s) – iespējami īsākais s ziņojuma apraksts
K(s) = |s|+C – īsākais apraksts, lai aprakstītu ziņu + konstante
Lai uzģenerētu nejaušu ciparu virkni:

S = x0, x1, x2, ... **Xi** pieredr kopai **[0,2n-1]**
Pat jau tiek pārtvertas ziņas **x0, ..., xm-1,** var uzminēt xm ar varbūtību **1/2n**
Par pamatu var kalpot fiziskie procesi, piemēram, termālās izmaiņas, vai kādas citas darbības



Šifru veidi

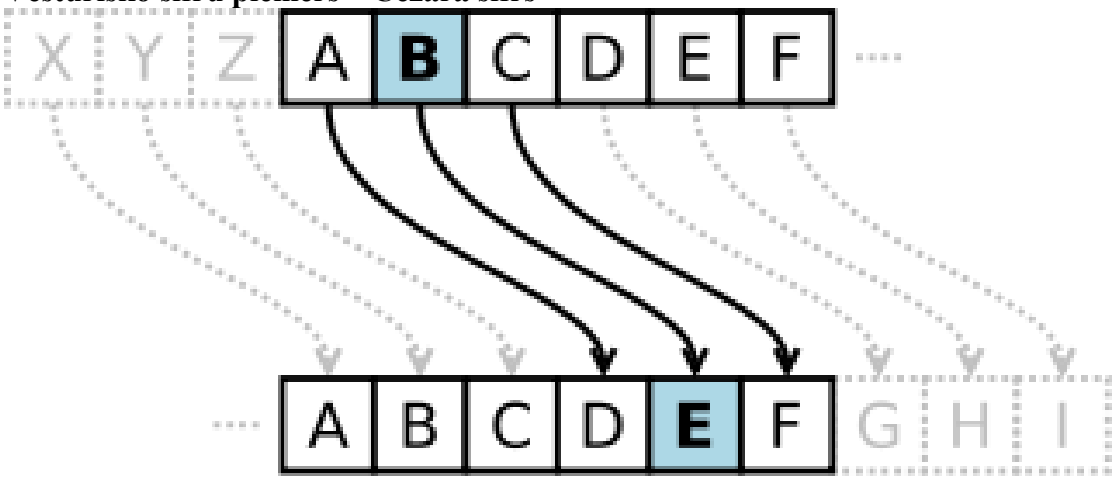
Simetriskie algoritmi – izmanto vienu atslēgu

Asimetriskie algoritmi – izmanto vairākas atslēgas

Plūstošie šifri – šifrē bitu pēc bita

Bloku šifri – dala informāciju pa blokiem

Vēsturisko šifru piemērs – Cēzara šifrs



C=E(P)=(P+K)mod(26)
P=D(C)=(C-K)mod(26)

Vēsturisko šifru piemērs – Viženēra šifrs

Key (s):	s	e	c	r	e	t	s	e	c	r	e	t
Plaintext (k):	d	a	s	i	s	t	g	e	h	e	i	m
Ciphertext (c):												

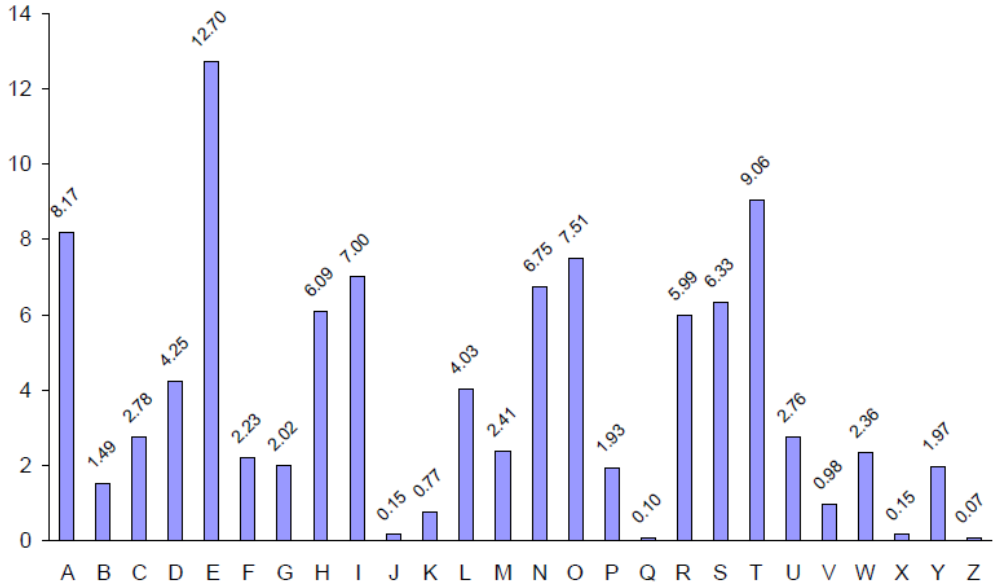
We can calculate the ciphertext with the formula:
c = (s + k) mod 26

21 = (18 + 3) mod 26

Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	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
Shift 0	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
1	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	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	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
4	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
5	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	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	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
10	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
11	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	k
12	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
13	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	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	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
19	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
20	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	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	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

Tiešo metožu vājums

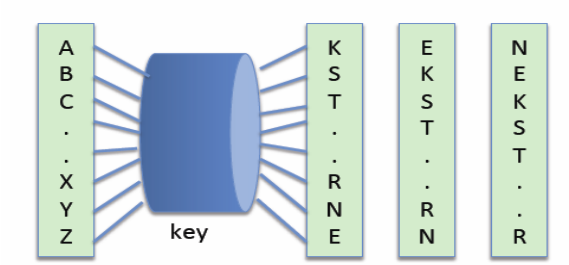
Valoda	Alfabēta burts/izmantošanas biežums %					
Angļu	E / 12,86	T / 9,72	A / 7,96	I / 7,77	N / 7,51	R / 7,03
Latviešu	A / 9,81	I / 7,70	S / 7,31	T / 5,11	E / 5,11	U / 5,02
Spāņu	E / 14,15	A / 12,90	O / 8,84	S / 7,64	R / 7,01	T / 6,95
Itāļu	I / 12,04	E / 11,63	A / 11,12	O / 8,92	N / 7,68	T / 7,07
Vācu	E / 19.18	N / 10,20	I / 8,21	S / 7,07	R / 7,01	T / 5,86
Franču	E / 17,76	S / 8,23	A / 7,86	N / 7,61	T / 7,30	I / 7,23
Krievu	O / 11,0	И / 8,9	E / 8,3	A / 7,9	H / 6,9	T / 6,0



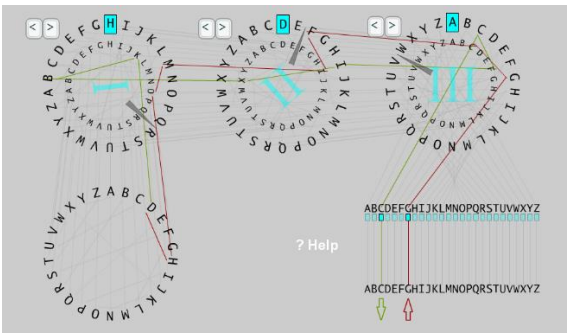
Avots:[fppt.com]

Rotoru mašīnas

Heberna mašina ar vienu rotoru



Enigma



Drošības par citām vēsturiskām metodēm būtiski neatšķiras!

Izglītības programma- Datorsistēmu tehniķis

Praktiskais darbs

Vārds uzvārds:

Tēma: *Kriptogrāfijas vēsturiskās metodes.*

Darba apjoms: *80 minūtes.*

Darba mērķis: *Zināšanu apguve par kriptogrāfijas vēsturiskajām metodēm.*

Darba prasības: *Aizpildīt atvēlētās vietas ar nepieciešamajām darbībām konkrētā uzdevumu veikšanai. Ja darbības ir vairākas, tad numurē tās.*

Darba uzdevumi:

1. Sastādi vienu kriptēšans metodi balstoties uz vēstures piemēriem un apraksti kriptēšanas pamatprincipus. (4*punkti*)

Metode: Apraksts: Slepenais ziņojums:

2. Apraksti atšifrējumu savai metodei un apraksti mīnusus konkrētajai kriptēšanas metodei. (4*punkti*)

Atšifrējums: Mīnusi: Priekšrocības:

3. Pilsētā ir 2 radio elektronikas veikali un 5 datortehnikas veikali, kuros var iegādāties datoru, cik veidos var iegādāties datoru? (4*punkti*)

Aprēķins: Atbilde:

   Atbilde: pavisam ir 2+5=7 iespējas.

4. Uz galda ir 5 planšetes, 2 telefoni un 3 portatīvie datori. Cik veidos var paņemt? (4*punkti*)

vienu telefonu: vienu planšeti vai vienu portatīvo datoru: vienu no ierīcēm? :

   Atbilde: a) 2; b)5+3=8; c) pavisam ir 3+2+5=10 iespējas.

5. C:/ diskā ir 32 direktorijas, no tām 14 ir teksta faili. Cik veidos var izvēlēties 1 vienu direktoriju, kas nav teksta fails no C:/ diska? (4*punkti*)

Aprēķins: Atbilde:

   Atbilde: pavisam ir 32-14=18 iespējas.

Darba vērtēšana:

Punkti	1-2p	3-4p	5-6p	7-8p	9-10p	11-12p	13-14p	15-16p	17-18p	19-20p
Balles	1	2	3	4	5	6	7	8	9	10

Par katru pareizu atbildi 2 punkti; Par katru daļēji pareizu atbildi 1punkts.

Drošs šifrs?

Herkofa (Kerckhoffs's) princips:

- Sistēmai ir jābūt praktiski, ja ne matemātiski neatšifrējamai.
- Sistēmai pašai pa sevi nav jābūt slepenai, izņemot atslēgu.
- Atslēgu ir jāvar noskaidrot un saglabāt bez rakstveida piezīmju palīdzības un arī maināmai pēc iesaistīto pušu gribas.
- Tai jābūt pārvietojamai, un tās izmantošanas funkcijas nevar pieprasīt vairāku cilvēku iesaistīšanos.
- Visbeidzot ir nepieciešams atcerēties, ka sistēmai ir jābūt pietiekoši vienkāršai, lai nebūtu jāatceras sarežģītus un garus noteikumus.

Pilnīgi noturīgi šifri

Vai pastāv šifri, kurus kriptoanalītiķis nevar atšifrēt, ja tam ir pieejams tikai šifrētais teksts?
Pirmais jautājumu formulēja Klods Šenons, praktiski risinājumam tuvu bija Džilberts Vernams
Vernama plūsmu šifrs (One Time pad):

Plaintext	1	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1
Keystream	0	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0
Ciphertext	1	0	1	0	1	0	0	1	1	1	0	0	0	1	1	1

(a) Encryption

Ciphertext	1	0	1	0	1	0	0	1	1	1	0	0	0	1	1	1
Keystream	0	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0
Plaintext	1	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1

(b) Decryption using an identical keystream

$$M=C=\{0,1\}^n$$

$$K = \{0,1\}^n \text{ random bitu virkne}$$

$$C := E(k,m) = k \otimes m$$

Saglabājot nosacījumus:

$$\forall m \in M, k \in K$$

$$D(k, E(k,m))$$

$$E(k,m)$$

Šenons nodefinēja – ka drošam šifram, nevajadzētu sniegt nekādu informāciju par pamattekstu

$$\forall m_0, m_{1,} \in M \quad (garums(m_0) = garums(m_1))$$

$$\forall c \in C$$

$$Varbūtība[E(k,m_0) = c] = Varbūtība[E(k,m_1) = c]$$

Simetriskie šifri: DES

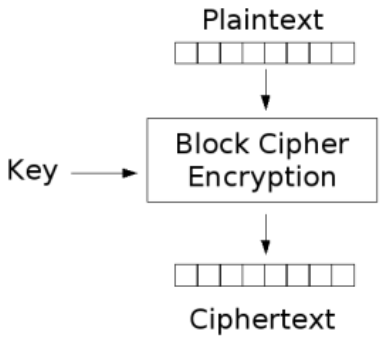
Pārejas šifrs starp vēsturiskajiem uz mūsdienu

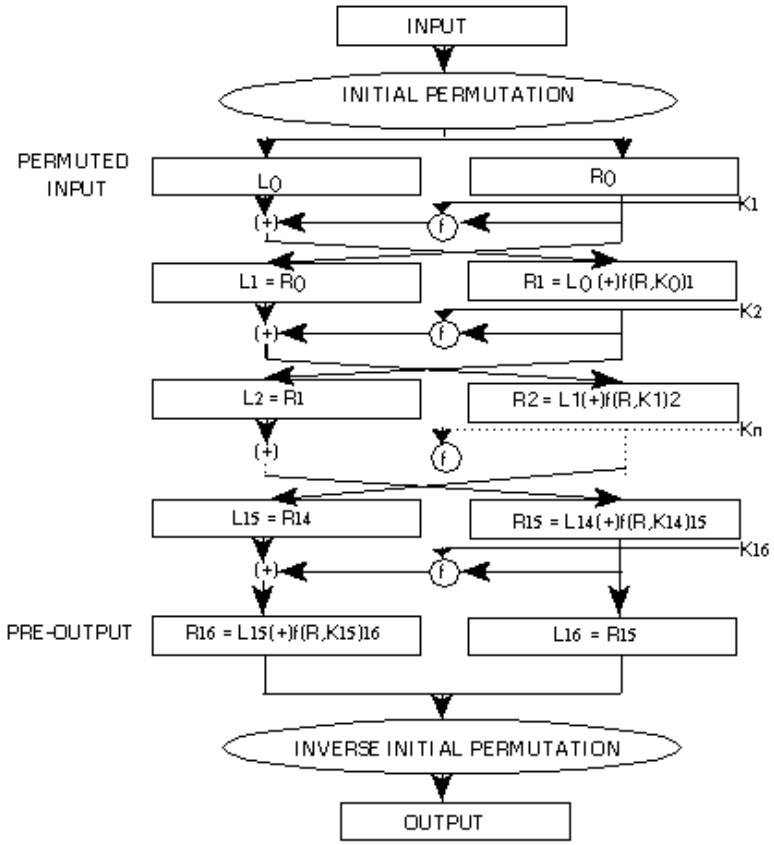
Bloku šifrs, kas apstrādā 64 bitu blokus

Strādā ar 56 bitu atslēgām

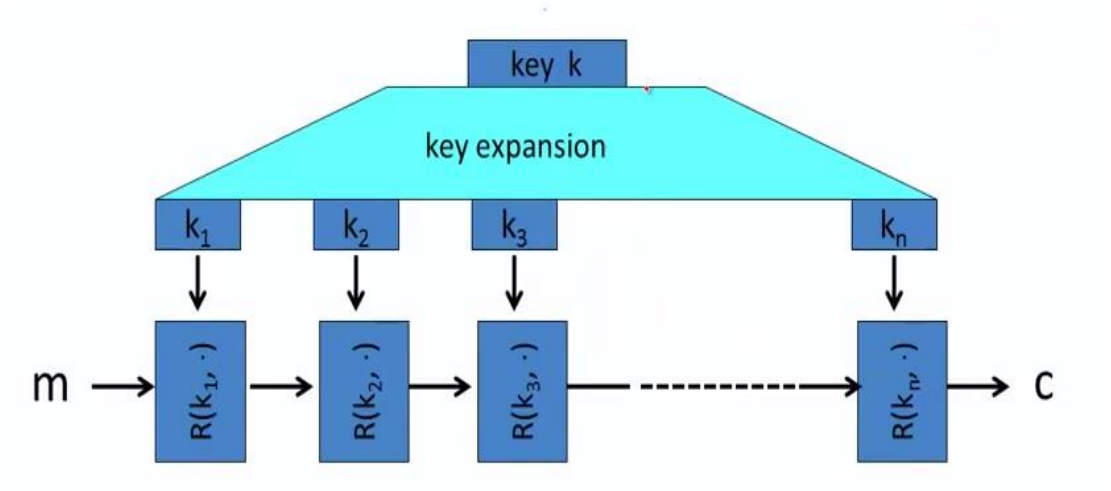
Pamatā izmanto :

- Izlīdzināšanu
- Sajaukšanu
- Aizvietošanu pārkārtošanu



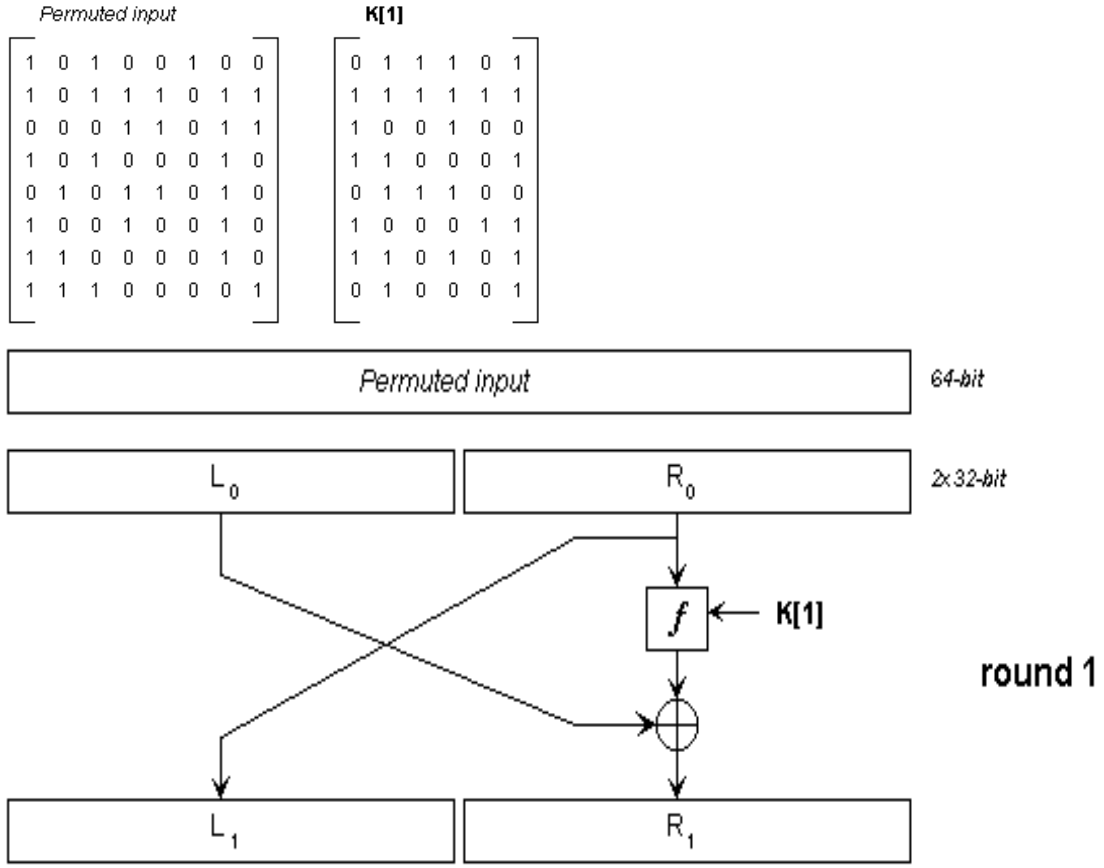


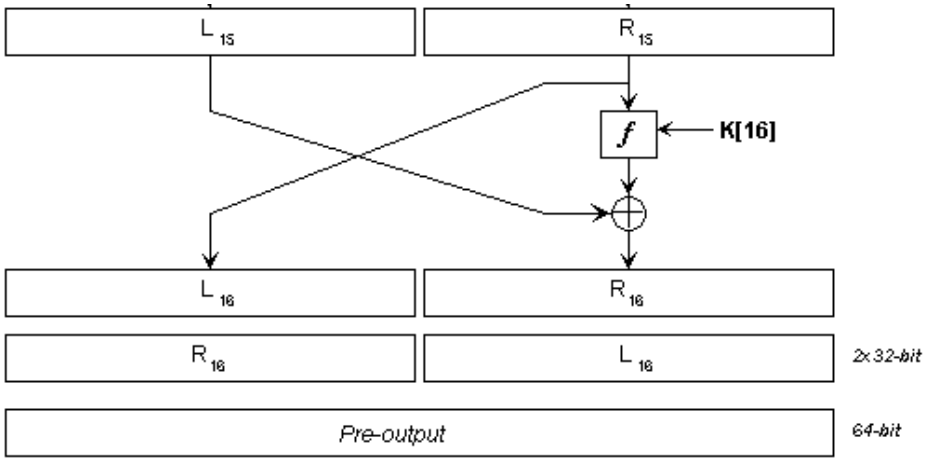
Atslēgu paplašināšanas princips



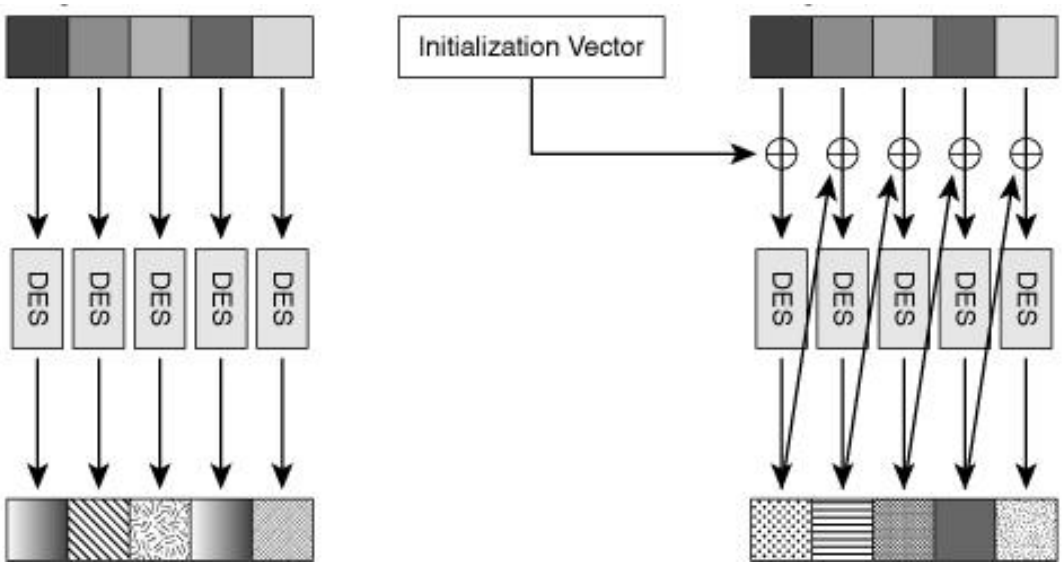
Bloku parasti apstrādā pa vairākiem raundiem, kur katrā raundā notiek R(k,m) funkcijas izpilde

Kad ir atslēgas raundi





DES režīmi



DES drošība

56 bitu gara atslēga, tas nozīmē atslēgu varianti ir 2^{56}

Ja dators veic vienu miljonu variantu sekundē – 2285 g.

Eksistē programmistiski ierobežojumi, kas sašaurina atslēgu kopu – 2^{56} jau ir 2^{40}

Atslēga	4 baiti	5 baiti	6 baiti	7 baiti	8 baiti
Lielie burti	0,6 sek	13 sek	6 min	2,3 h	2,5 dienas
Lielie burti un cipari	1,8 sek	2 min	37 min	23 h	34d
Burti un cipari	16 sek	16 min	17 h	42 d	7 gadi
Klaviatūras simboli	1,5 min	2,2h	8,6d	2,3 d	211 gadi
Visi ASCII	1,3 h	14 d	9 g	2400 g	590 000 g

1997. gadā atslēga tika atrasta 96 dienās. Vēlāk 1998. gada februārī šī pati metode ļāva atslēgu iegūt 41 dienā (pielietojot sadalīto aprēķinu metodi

1998, gadā tika izveidots speciāls dators (izmaksas 250 000 USD), kurš šo pašu pārlasi veica 56 stundās.

Desmitnieku sistēma				Divnieku sistēma	
Reizinātajs	Apzīmējums	Nozīme	Vērtība	Reizinājums	Vērtība
10^3	k	Kilo	1000	2^{10}	1024
10^6	M	Mega	1000 000	2^{20}	1 048 576
10^9	G	Giga	1000 000 000	2^{30}	1 073 741 824
10^{12}	T	Tera	1000 000 000 000	2^{40}	1 099 511 627 776
10^{15}	P	Peta	1000 000 000 000 000	2^{50}	1 125 899 906 842 624
10^{18}	E	Exa	1000 000 000 000 000 000	2^{60}	1 152 921 504 606 846 980
10^{21}	Z	Zetta	1000 000 000 000 000 000 000	2^{70}	1 180 591 620 717 411 300 000

Izglītības programma- Datorsistēmu tehniķis

Praktiskais darbs

Vārds uzvārds:

Tēma: *Reizināšanas likums kriptogrāfijā.*

Darba apjoms: *80 minūtes.*

Darba mērķis: *Zināšanu apguve par reizināšanas likumu kriptogrāfijā.*

Darba prasības: *Aizpildīt atvēlētās vietas ar nepieciešamajām darbībām konkrētā uzdevumu veikšanai. Ja darbības ir vairākas, tad numurē tās.*

Darba uzdevumi:

1. Doti 3 burti A;B;C. Cik dažādu vārdu kodu var izveidot no šiem burtiem, ja burti nedrīkst atkārtoties? (4*punkti*)

Aprēķins: Atbilde:

   Atbilde: pavisam ir 3*2*1=6 iespējas.

2. Komplektējot datoru, ir 4 vienas paaudzes atšķirīgas sistēmas plates un četri atšķirīgi tās pašas paaudzes procesori. Cik veidos iespējams izvēlēties komplektāciju datoram no šīm komponentēm? (4*punkti*)

Aprēķins: Atbilde:

   Atbilde: pavisam ir 4*4=16 iespējas.
3. Cik dažādu 4 cipara nepāra skaitļu var izveidot no cipariem 1;2;3;4;5, ja skaitlī (4*punkti*)

a) cipari nedrīkst atkārtoties: b) cipari drīkst atkārtoties:

Atbilde: a)4*3*2*3=72 b)5*5*5*3=375

4. Cik dažādu 3 cipara skaitļu var izveidot no cipariem 0;1;2;3;4;5, ja skaitlī (4*punkti*)

a) cipari nedrīkst atkārtoties: b) cipari drīkst atkārtoties: c) cipari nedrīkst atkārtoties, un skaitlis dalās ar 10: d) cipari nedrīkst atkārtoties, un skaitlis dalās ar 5?:

Atbilde: a) 5*5*4=100 b) 5*6*6=180 c) 5*4*1=20
d) 4*4*1+5*4*1=20+16=36.

5. Cik liels skaitļošanas potenciāls simbolu noteikšanai ir procesoram, kuram ir 4 kodoli un 4Ghz takts frekvence? (4*punkti*)

Aprēķins: Atbilde:

Atbilde: pavisam ir $4*4*10^9/8=2*10^9$.

Darba vērtēšana:

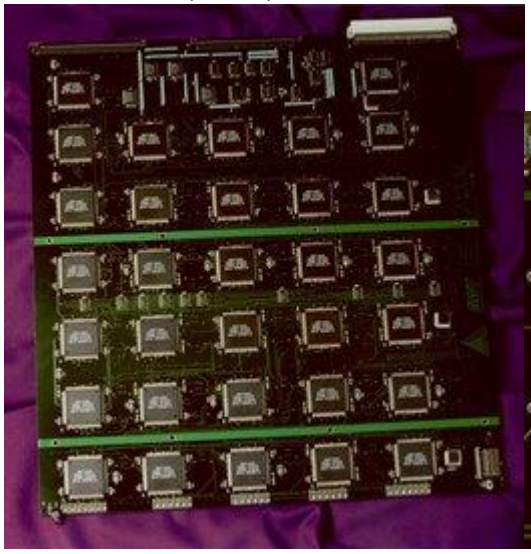
Punkti	1-2p	3-4p	5-6p	7-8p	9-10p	11-12p	13-14p	15-16p	17-18p	19-20p
Balles	1	2	3	4	5	6	7	8	9	10

Par katru pareizu atbildi 2 punkti; Par katru daļēji pareizu atbildi 1punkts.

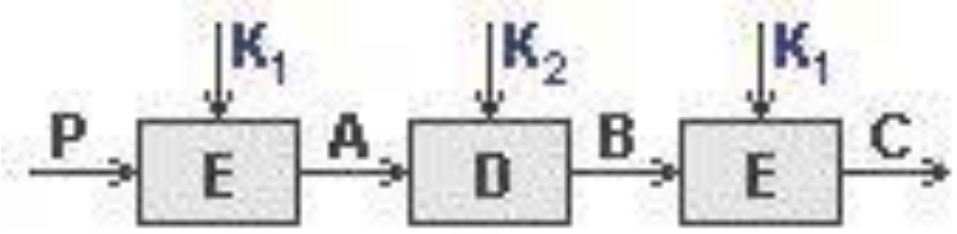
Dekriptēšanas metodes

Deep crack

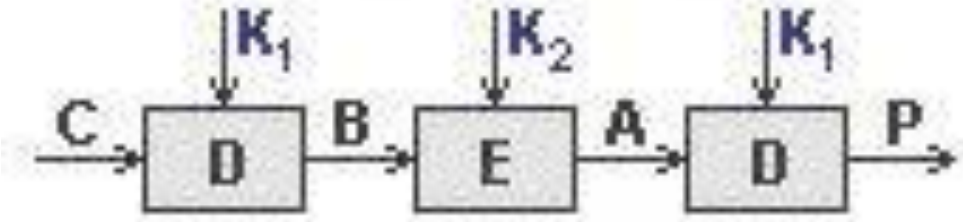
Ideja (M. Wiener) – ņemam 1 miljonu mikroshēmu, kas katra veic pārlases noteiktu posmu- mums visam vajag tikai 20 stundas.
1999. gada janvārī pielietojot Deep Crack kopā ar sadalīto aprēķinu shēmu, atslēga tika iegūta 22 stundās un 15 minūtēs.
DES tika paziņots par nedrošu un vairs nav ieteicams lietošanai un atrastas tādas alternatīvas kā, AES, 3DES



3DES



Šifrēšana



Dešifrēšana

3DES drošība jau ir 2^{128}
Ir drošāks, bet ļoti lēns algoritms

Ko nozīmē lēns?

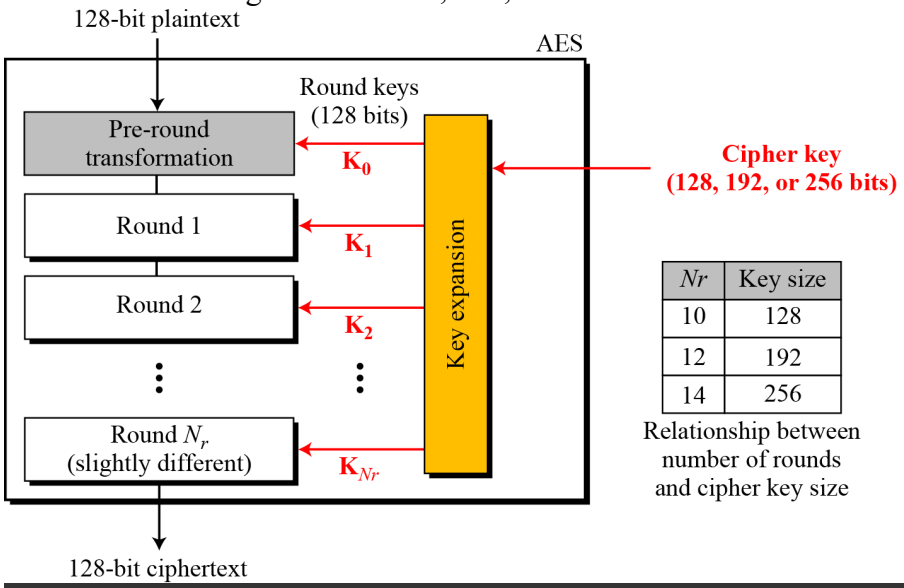
AMD Opteron, 2.2 GHz (Linux)		
Šifri	**Bloka/atslēgas lielums**	**Ātrums(MB/sec)**
RC	**4**	**126**
Salsa	**20/12**	**643**
Sosemanuk	**4**	**727**
3DES	**64/168**	**13**
AES-128	**128/128**	**109**

AES

Advanced Encryption Standard (AES) izveidojis National Institute of Standards and Technology (NIST)

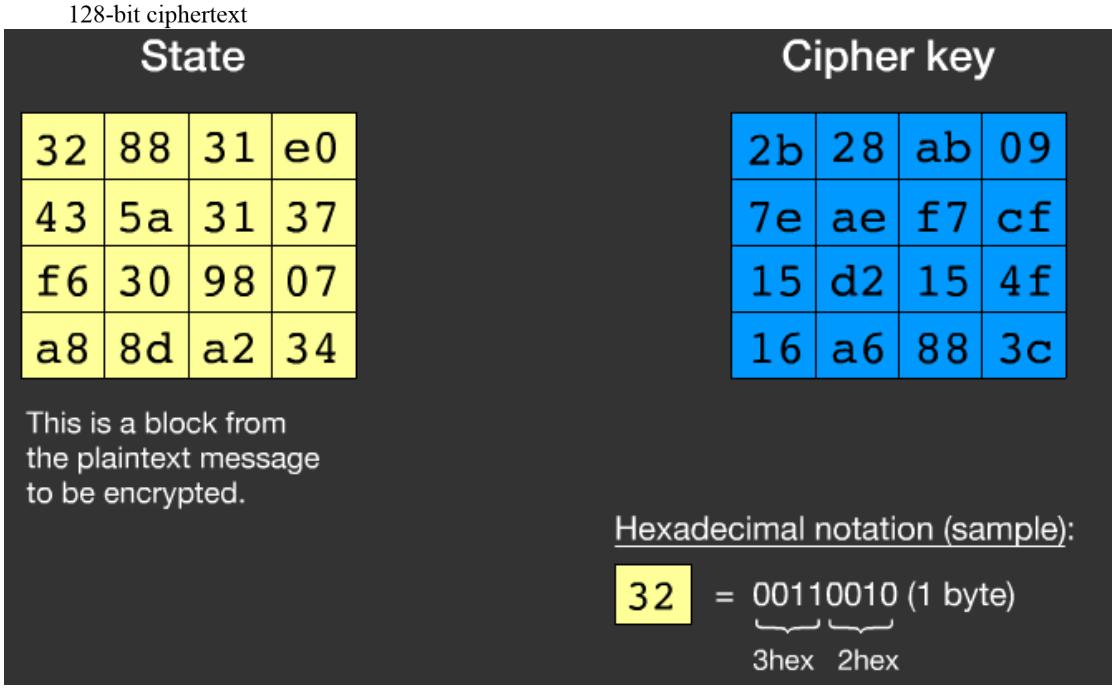
Pastāv dažādi varianti ar 10, 12, 14 raundiem

Pastāv dažādi atslēgu varianti 128, 192, 256



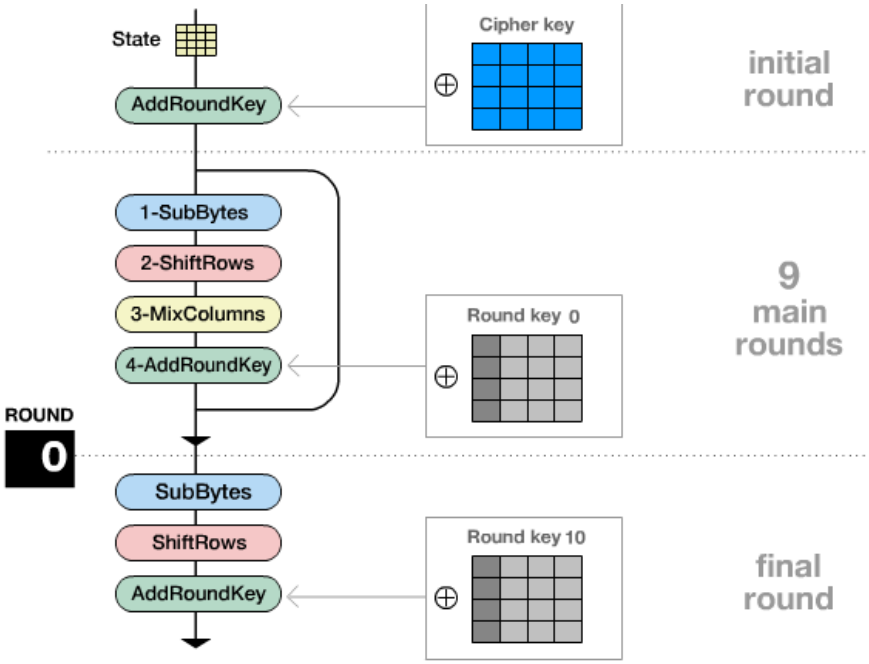
Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size



Tālāk notiek divi atsevišķi procesi: bloka šifrēšana un atslēgas sadalīšana

Šifrēšanas process



Simetriskās šifrēšanas problēmas

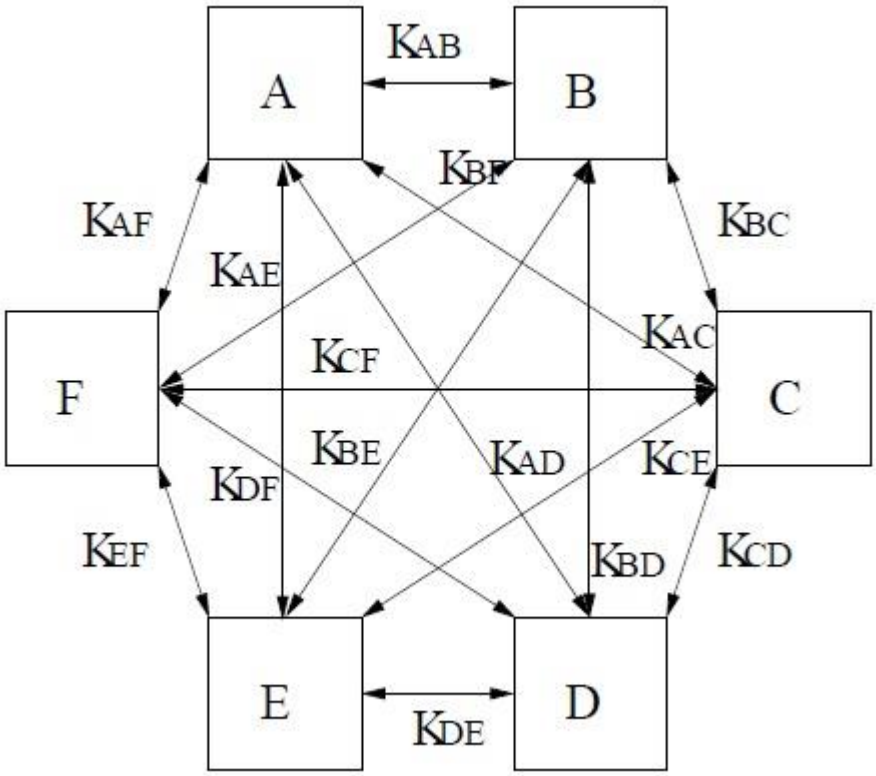
Milzīgākā problēma atslēgu apmaiņa

Atslēgu ģenerēšanas problēma (zinot algoritmu un visus iepriekšējos skaitļus, nav iespējams noteikt nākošo?)

Atslēgas uzglabāšana

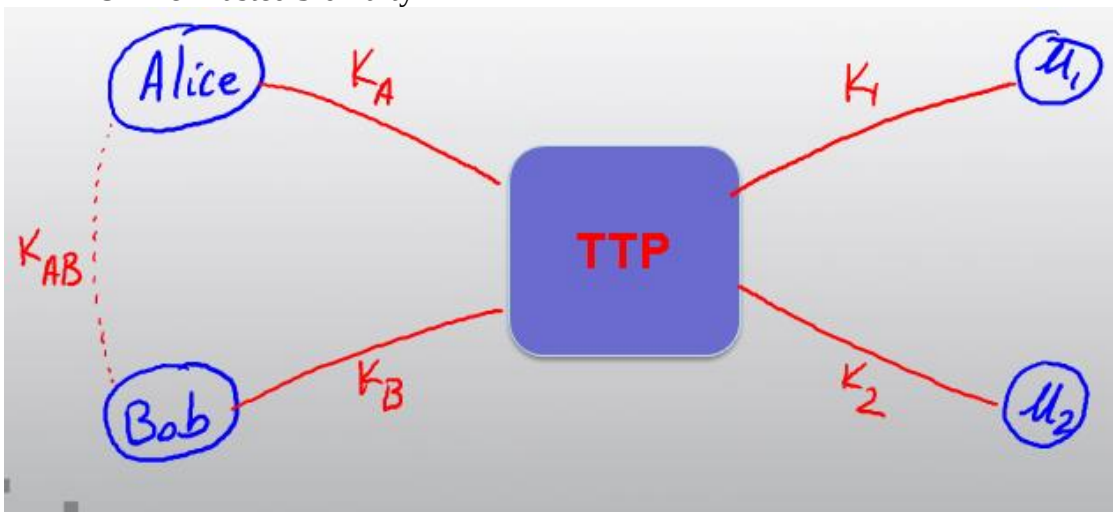
Ar slepenām atslēgām arī nav vieglāk

Problēma: daudz lietotāju. Simetriskās šifrēšanas gadījumā vajag daudz atslēgu.

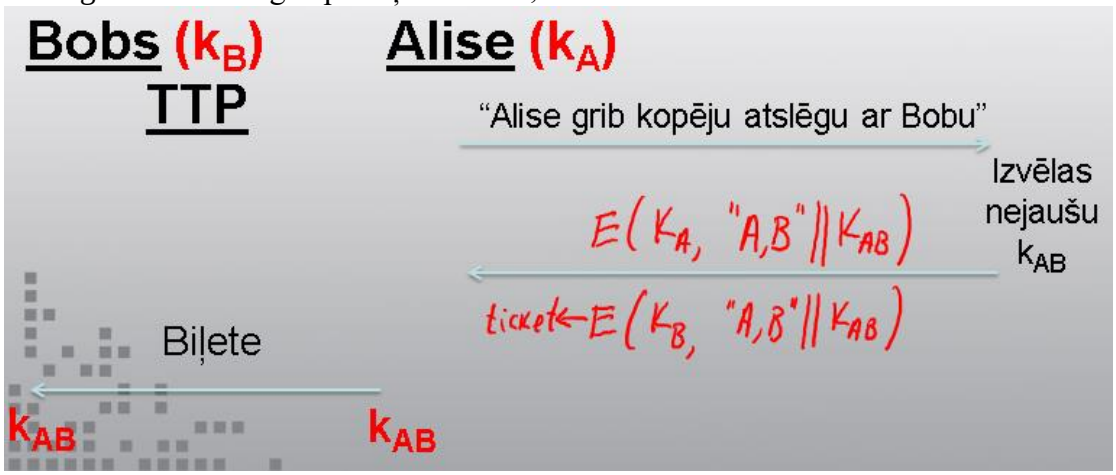


n(n-1)/2 atslēgas tiks izmantotas sistēmā

Mazliet labāks risinājums
TTP - Online Trusted 3rd Party

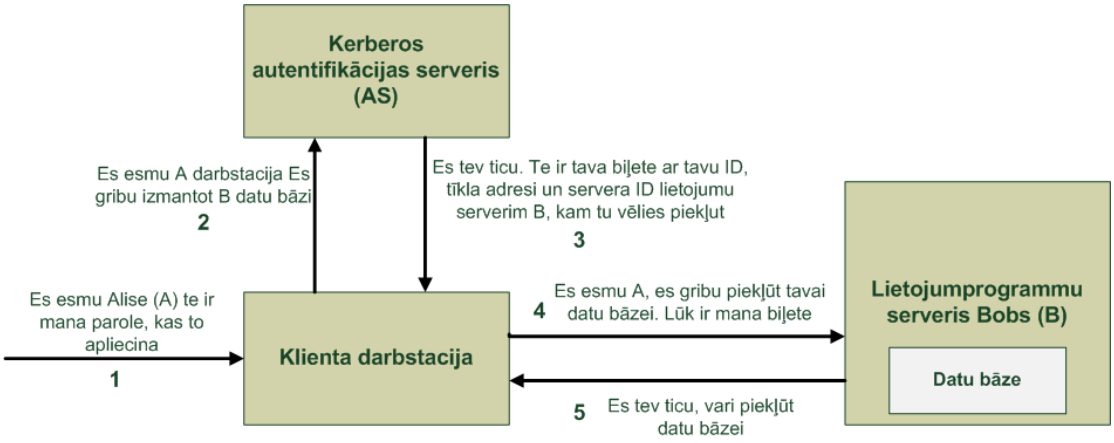


Iesaistām trešo pusi, kas apmaina atslēgu, un katram jāatceras tikai vienu atslēgu.
Piemērs:
Alise grib veikt atslēgu apmaiņu ar Bobu, lai nenotiktu noklausīšanās:



Atslēgu ģenerēšana no malas
Brīdī, kad Alise ar Bobu mainās atslēgām, uzbrucējs redz:
E(kA, "A, B" ll kAB); E(kB, "A, B" ll kAB)
Uzbrucējs neiegūst nekādu info par kAB TTP vajadzīgs katrā atslēgu apmaiņā, zina visas sesiju atslēgas. Nav aizsargāts pret aktīvajiem uzbrukumiem, piemēram, replay attack.

Kerberos metode:
atslēgu izplatīšanas un autentifikācijas serviss, kas izstrādāts Masačūsetsas Tehnoloģiju institūtā
Pašlaik lietošanā eksistē Kerberos 4 un Kerberos 5 versijas.



Vienvirziena funkcijas

Vienvirziena funkcija ir matemātiskas funkcijas, kuras daudzreiz vienkāršāk ir izrēķināt vienā virzienā (Uz priekšu) nekā pretēji (atpakaļ).
Lūkas (trapdoor) vienvirziena funkcija ir vienvirziena funkcija, kuras inversais apēķins ir vienkāršs, ja tiek dota noteikta informācija citādi – sarežģīts.
-Lielo skaitļu reizinājumi N=PxQ N~2^{664} P~Q
Lai N sadalītu reizinātājos jāveic 10^{23} operācijas.
-Diskrēto logaritmu shēmas

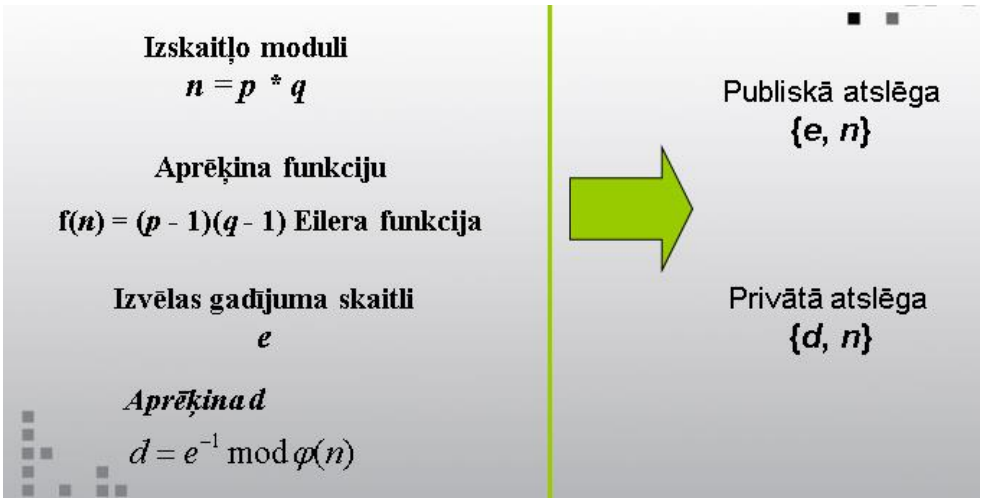
Ja A, N ir veseli skaitļi, kur $1 \leq A < N$, tad viegli aprēķināt funkciju

$f_{A,N} = A^x \pmod N$, kur x – vesels skaitlis $1 \leq x \leq N-1$.

Tai pašā laikā, zinot A, N, y, ir ļoti grūti atrast tādu x, lai $A^x \bmod N = y$.

Šajā gadījumā pie A = 2^{664} un N = 2^{664} x atrašanai ir nepieciešamas 10^{26} operācijas.

RSA
Autori: **R**onald L. Rivest, Adi **S**hamir, Leonard **A**dleman
Asimetriskā kriptosistēma, kas izmanto 2 atslēgas:
-Publiskā atslēga:
šifrēt ziņojumu;
verificēt parakstu.
-Privātā atslēga:
atšifrēt ziņojumu;
ģenerēt parakstu.
Darbības princips



Piemērs:
p = 61 – pirmais pirmskaitlis (jātur slepenībā vai arī ir jāiznīcina)
q = 53 – otrais pirmskaitlis (jātur slepenībā vai arī ir jāiznīcina)
n = p*q = 3233 – reizinājums (publiskojam)
φ = (61-1)(53-1) = 3120
e = 17 – publiskā eksponente (atslēga)
d = 2753 – privātā atslēga (jātur noslēpumā)

RSA publiskā atslēga {e, n}
n modulis, nenegatīvs vesels skaitlis,
e publiskā eksponenta, nenegatīvs gadījuma vesels skaitlis.
Modulis n ir divu atšķirīgu pirmskaitļu p un q reizinājums.
Publiskā eksponenta e ir vesels skaitlis, kas mazāks par n un ir relatīvs pirmskaitlis reizinājumam (p-1) * (q-1)

RSA privātā atslēga {d, n}
n modulis, nenegatīvs vesels skaitlis,
d privātā eksponenta, nenegatīvs vesels skaitlis.

Modulis n ir tas pats, kas iepriekš aprakstītā publiskā atslēgā.
Privātā eksponenta d ir pozitīvs skaitlis, kas mazāks par n un apmierina vienādību:

$$d * e \bmod \phi = 1$$

RSA šifrēšana
Ieeja: (n,e) RSA publiskā atslēga,
m ziņojuma attēlojums – skaitlis intevālā (0,n-1)
Izeja: c kriptogrammas attēlojums –skaitlis intervālā (0,n-1)
Kļūdas: "ziņojuma attēlojums ir ārpus pieļaujamā intervāla"

1.Ja ziņojuma attēlojums m neietilpst noteiktajā intervālā (0,n-1), tad tiek paziņots par kļūdu un algoritma izpilde tiek apstrādināta.
2.Kriptogrammas aprēķins: $c\text{-}m^e \bmod n$
3.Izejā tiek iegūta kirptogramma c.

RSA atšifrēšana

Ieeja: K RSA prvātā atslēga (n,d),
c kriptogrammas attēlojums –skaitlis intervālā (0,n-1
Izeja: m ziņojuma attēlojums –skaitlis intervālā (0,n-1)
Kļūdas: "kriptogramma attēlojums ir ārpus pieļaujamā intervāla"

1.Ja kirptogrammas attēlojums c neietilpst noteiktajā intervālā (0,n-1)
2.Ziņojuma teksta aprēķins:
3.Izeja tiek iegūts ziņojums m. $m=c^d \bmod n$

RSA ar zemu eksponenti
Lai paātrinātu RSA šifrēšanu izvēlas zemu
e: c = me (mod N)

Minimālā vērtība: e=3 (gcd(e, □(N)) = 1)
X3 Mod M = 3 reizinājumi
Ieteicamā vērtība ar ko sākt: e=65537=216+1
Šoreiz jau 17 reizinājumi
Faktorizācija – sadala skaitli mazākos skaitļos, kurus reizinot tiek iegūts sākotnējais skaitlis. Tad iegūstam ātru šifrēšanu, bet lēnu atšifrēšanu

Daži izmantošanas specifikas uzbrukumi
Laika uzbrukumi: (Kocher 97)
Laiks, lai izskaitļotu cd (mod N) ļauj izteikt d

Jaudas uzbrukums (Kocher 99)
Viedkartes strāvas patēriņš cd (mod N) laikā ļauj noteikt d

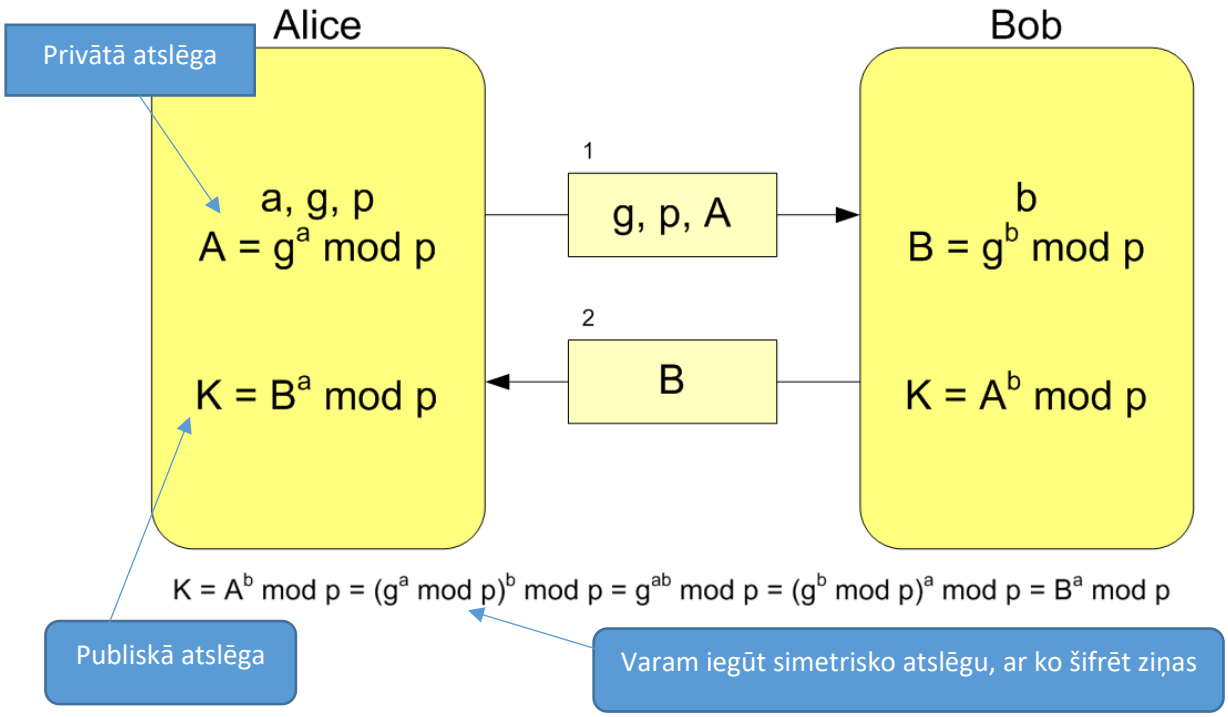
Kļūdu uzbrukums
Šifrēšanas uzbrukumi cd (mod N) laikā ļauj izrēķināt d (pietiek ar 1 kļūdu)

RSA atslēgu ģenerēšanas problēma
OpenSSL RSA atslēgu ģenerēšana:
prng.seed(seed)
p = prng.generate_random_prime()
prng.add_randomness(bits)
q = prng.generate_random_prime()
N = p*q
Pieņemot, ka sākumā ģenerē mazas vērtības
Daudzām sistēmām sakrīt p, bet ir savādāks q
N1,N2:ņemot RSA atslēgas no dažādām ierīcēm ⇒ gcd(N1,N2) = p

El-gamala paraksta shēma
Izvēlamies privāto un publisko atslēgu pāri
-P (pirmskaitlis) un
-G (vesels skaitlis), G<P
izvēlas gadījuma rakstura veselu skaitli X (tā būs privātā atslēga) (1< X<= P-1)
rēķinām publisko atslēgu Y (to mēs nosūtām visiem iespējamiem dokumenta saņēmējiem) Y=GXmodP
lai parakstītu ziņojumu M, rēķina tā jaucējkoda vērtību m = h(M) 1< m < (P-1)

tad ģenerējam gadījuma rakstura skaitli K (1 < K < (P-1) ar prasību, ka tam un (P-1) nav kopīgu dalītāju (ir savstarpēji pirmskaitļi)
Aprēķina a=GKmodP
zinot privāto atslēgu X , aprēķina b no vienādojuma m = X a + Kb(mod (P-1))
skaitļu pāris a un b veido dokumenta M elektronisko parakstu S = (a,b)
informācija (m, a,b) tiek nodota adresātam, savukārt (X, K) tiek turēta slepenībā

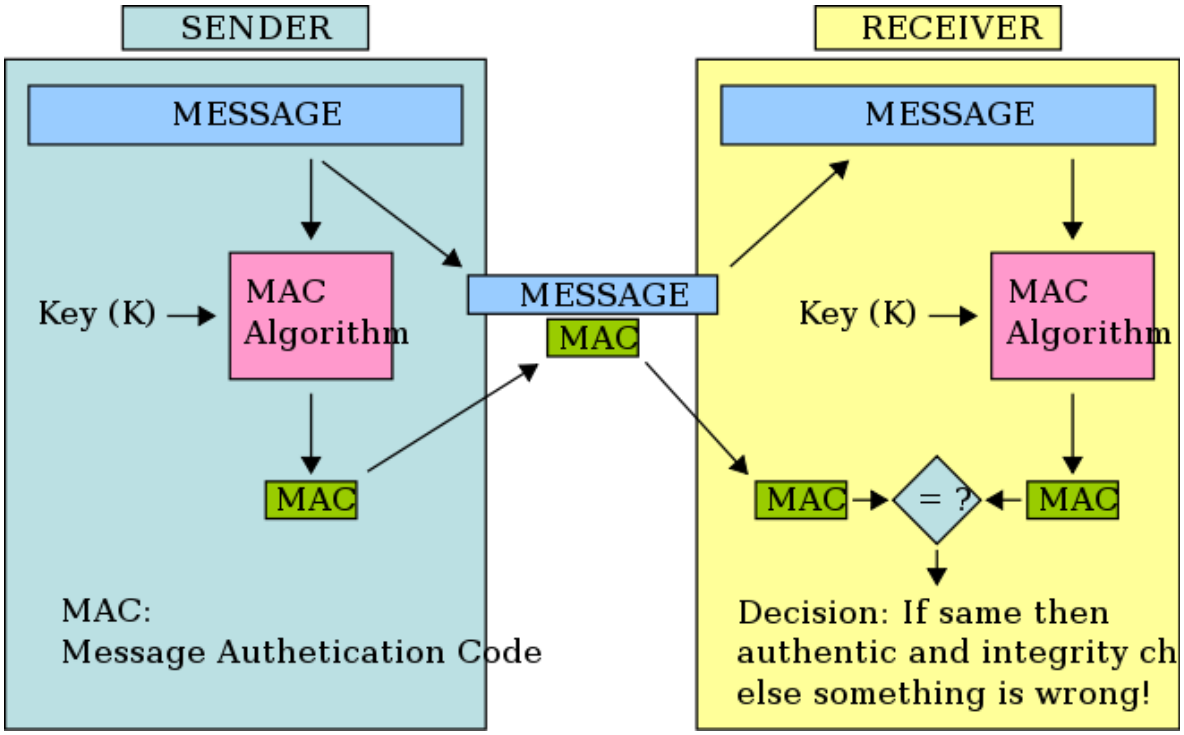
Cēlies no Diffie-Helman protokola



EL-GAMALA paraksta pārbaude
saņēmējs iepriekš zina P un Y.
sūtījuma saņēmējs aprēķina ziņojuma M hash vērtību m= h(M)
aprēķina vērtību A = Ya ab (mod P)
ziņojuma paraksts tiek atzīts par patiesu tad un tikai tad, ja A = Gm(mod P)

Pozitīvais – nepiemīt iepriekš minētais RSA trūkums
Trūkums – paraksts vidēji 1,5 reizes garāks nekā RSA

Ziņu integritāte – MAC

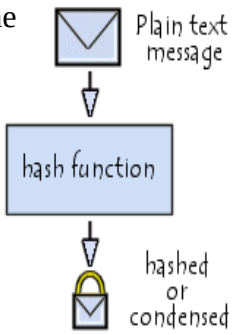


V(k,m,MAC)=Jā/Nē

Pie mazākām x kopas izmaiņām, y kopa mainās radikāli, turklāt neprognozējami

Hašēšana – pārveido kopu kopā ar daudz mazāku iespējamo stāvokļu skaitu

No neierobežota garuma virknes tiek atgriezta noteikta garuma virkne



Vienvirziena funkcija

Jūtīga pret izmaiņām kopā X
(pat viena simbola izmaiņas rada lielas izmaiņas):
Ļauj pārliecināties, ka ziņojums nav mainīts
Ļauj pārliecināties, ka sūtītājs nav cits

Divas jaucējkoda vērtības nedrīkst sakrist

MD5
Apstrādā ziņojumu pa 512 bitu datu blokiem.
Katru bloku apstrādā četros ciklos ar 16 soļiem katrs.
Izejā iegūst 128 bitu hash vērtību.
Kolīziju iegūšanas teorētiska sarežģītība 2^{64}.
Izdod 128 bitu ziņojuma vērtību, apstrādā pakāpeniski blokos pa 512 bitiem

SHA-1 (Secure Hash Algorithm)
Apstrādā ziņojumu pa 512 bitu datu blokiem.
Katru bloku apstrādā iekš ciklā ar 80 soļiem.
Izejā iegūst 160 bitu hash vērtību.
Kolīziju iegūšanas teorētiska sarežģītība 2^{80}

MD5 un SHA-1 analīze

Aizsardzība

SKA–1 profils par 32 bitiem garāks par MD5 profilu. MD5 atslēgas iespējamās variācijas – 2128, bet SHA – 2160 (SHA–1 drošāks).

Ātrums

Algoritms SHA–1 ietver sevī 80 darbības soļus un datu apstrāde notiek 160 bitu buferī. Savukārt, algoritms MD5 ietver sevī 64 darbības soļus, un datu apstrāde notiek 128 bitu buferī. Tātad, pie vienādas aparatūras, algoritms SHA–1 izpildīsies lēnāk.

Vienkāršība

Abi algoritmi ir vienkārši realizējami – nav nepieciešamas lielas aplikācijas un liels tabulu daudzums.

Brute force: bruteforce algoritmi uzmin diezgan veikli – ejam cauri vārdnīcai, ņemam katru vārdu, aizvietojot burtus ar iespējamajiem aizvietotājiem (pamēģinām "a", tad "@") un liekot klāt priekšā un/vai beigās vienu vai divus populārākos simbolus. Iespējamo kombināciju skaits ir relatīvi mazs. Pie kam, šādu paroli, ja tā regulāri jāmaina, atcerēties nav dikti viegli. Nāksies arī pasvīst, ja būs jāievada uz mobilajām ierīcēm.

Birthday attack

Birthday ir kriptogrāfisko uzbrukumu veids, kas izmanto matemātiku dzimšanas dienas paradoksam, izmantojot laika un telpas sakarības. Dzimšanas dienas paradoksu mēs varam raksturot, no n nejauši izvēlētiem cilvēkiem, kādiem no viņiem sakritīs dzimšanas diena.

Tātad attiecībā uz Hash funcijām, ja funkcija dod dažādu vērtību n ar vienādu varbūtību un n ir pietiekami liels, tad pastāv varbūtība, ka diviem dažādiem argumentiem x1 un x2 būs vienādas funkciju vērtības f(x1) = f(x2), šī parādība pazīstama arī kā kolīzijas.

Social Engineering: Bobs- "Sveika Suzija". Mans vārds ir Bobs un esmu no IT departamenta. Mēs tagad instalējam aizsardzības papildinājumu uz jūsu datora, bet mēs nevaram pieslēgties lietotāju datubāzei un papildināt lietotāju informāciju. Vai jūs nevarētu palīdzēt man pasakot savu ieejas paroli, pirms mans boss man norauj ādu pār acīm, man šodien ne pārāk veiksmīga diena, ja saprotat, ko es ar to gribu teikt. ☺

Rainbow table - ir milzīgs saraksts ar uzkaukulētām jaucējkods vērtībām priekš visām iespējamām simbolu kombinācijām. Paroles jaucējkods ir matemātisks algoritms, kurš pārveidots par kaut ko nenoteiktu.

Piemērs: Vārds "cheese" caur md5 algoritmu, iznākums fea0f1f6fede90bd0a925b4194deac11

Izglītības programma- Datorsistēmu tehniķis

Praktiskais darbs

Vārds uzvārds:

Tēma: *Kriptogrāfija.*

Darba apjoms: *2 stundas.*

Darba mērķis: *Zināšanu apguve par kriptogrāfiju.*

Darba prasības: *Aizpildīt atvēlētās vietas ar nepieciešamajām darbībām konkrētā uzdevumu veikšanai. Ja darbības ir vairākas tad numurē tās.*

Darba uzdevumi:

2. Aprēķināt dotos uzdevumus. (6*punkti*)

5!-4!=:
Atbilde: 5!-4!=120-24=96

3!+4!=:
Atbilde: 3!+4!=6+24=30
7!:6!=:
Atbilde: 7!:6!=7
9!:10!=:
Atbilde: 9!:10!=0.1
8!:6!=:
Atbilde: 8!:6!=7*8=56
12!:10!=:
Atbilde: 12!:10!=11*12=132

2. Aprēķināt dotos uzdevumus. (3*punkti*)

Cik dažādos veidos 5 datorus var novietot vienā rindā?:

Atbilde: 5!=5*4*3*2*1=120 veidos.

Cik dažādos veidos datoram var sastādīt 7 programmu startēšanās sarakstu?:

Atbilde: 7!=7*6*5*4*3*2*1=4050 veidos.

Datorā ir 5 lietotāji. Cik veidos 5 izveidot lietotājus, ja administratora profili drīkst piešķirt tikai 2 no viņiem?:

Atbilde: 2*4!= 2*4*3*2*1=48 veidos.

3. Aprēķināt dotos uzdevumus. (3*punkti*)

Noskaidro, cik dažādos veidos var sastādīt viena datora cieto disku komplektāciju, ja pastāv 10 atšķirīgi diski un datorā ir tikai paredzētas 4 disku vietas:

Atbilde: A_{10}^{4}=10*9*8*7=90*63=5040.

Pilsētā ir piecas e-sports komandas, kas cīnās par zelta, sudraba, bronzas medaļām. Cik veidos var sadalīt medaļas starp šīm komandām?:

Atbilde: A_{5}^{3}=5*4*3=60.

Cik dažādu durvju kodu var izveidot no dotiem 22 burtiem, ja kods sastāv 4 dažādiem burtiem, kuri jānospiež secīgi?:

Atbilde: A_{22}^{4}=22*21*20*9=175 560.

4. Aprēķināt dotos uzdevumus. (8*punkti*)

Šaha turnīrā piedalījās 15 šahisti, un katrs izspēlēja ar katru vienu partiju. Cik pavisam partiju izspēlēja?:

$$Atbilde: C_{15}^{2} = \frac{15!}{2! \cdot (15-2)!} = \frac{13!\,14 \cdot 15}{2! \cdot (13)!} = 105$$

Cik veidos no 10 skolēniem var izvēlēties 3 skolēnus braucienam praksē uz Vāciju?:

$$Atbilde: C_{10}^{3} = \frac{10!}{3! \cdot (10-3)!} = \frac{7! \cdot 8 \cdot 9 \cdot 10}{3! \cdot (7)!} = 120$$

Jauniešu grupā ir 10 meitenes un 5 zēni.

Cik veidos var izvēlēties braucienam uz koncertu:

1) vienu jaunieti;

2) trīs meitenes;

3) trīs zēnus un 2 meitenes?:

Atbilde:1) 10+5=15 veidos

2) $C_{10}^{3} = 120$ veidos

3) $C_{5}^{3} \cdot C_{10}^{2}$ =10*45=450 veidos

Darba vērtēšana:

Punkti	1-2p	3-4p	5-6p	7-8p	9-10p	11-12p	13-14p	15-16p	17-18p	19-20p
Balles	1	2	3	4	5	6	7	8	9	10

Par katru pareizu atbildi 2 punkti; Par katru daļēji pareizu atbildi 1punkts.

Izglītības programma- Datorsistēmu tehniķis

Praktiskais darbs

Vārds uzvārds:

Tēma: *Kriptogrāfija.*

Darba apjoms: *2 stundas.*

Darba mērķis: *Zināšanu apguve par kriptogrāfiju.*

Darba prasības: *Aizpildīt atvēlētās vietas ar nepieciešamajām darbībām konkrētā uzdevumu veikšanai. Ja darbības ir vairākas, tad numurē tās.*

Darba uzdevumi:

5. Nodemonstrēt, kā ar operētājsistēmas Windows kritpēšanas rīku tiek šifrēti faili. (1*punkti*)
6. Nodemonstrēt, kā operētājsistēmas Windows šifrētus failus var dešifrēt. (2*punkti*)
7. Apraksti, kā šifrēt Windows operētājsistēmas failus ar tās iebūvētajiem rīkiem. (2*punkti*)

Apraksts: Kādēļ nepieciešams to darīt?:

8. Apraksti 3 alternatīvas šifrēšanas programmatūras. (15*punkti*)

Programmatūra1 Nosaukums: Šifrēšanas pakāpe: Tehniskā specifikācija: Programmatūras noslogotība: Atšifrēšanas metode: Programmatūra2 Nosaukums: Šifrēšanas pakāpe: Tehniskā specifikācija: Programmatūras noslogotība: Atšifrēšanas metode: Programmatūra3 Nosaukums: Šifrēšanas pakāpe: Tehniskā specifikācija: Programmatūras noslogotība: Atšifrēšanas metode:

Darba vērtēšana:

Punkti	1-2p	3-4p	5-6p	7-8p	9-10p	11-12p	13-14p	15-16p	17-18p	19-20p
Balles	1	2	3	4	5	6	7	8	9	10

Par katru pareizu atbildi 2 punkti; Par katru daļēji pareizu atbildi 1punkts.