

Kriptologija

Vilius Stakėnas

VU MIF

2014

1. Įvadas

Duomenų apsaugos uždaviniai

Šiuolaikinę kriptografiją „pagimdė“ kompiuteriniai tinklai.

Duomenų apsaugos tikslai:

- duomenų slaptumas (konfidencialumas);
- duomenų vientisumas (integralumas);
- duomenų šaltinio autentiškumo užtikrinimas;
- vartotojo autorizavimas (naudojimosi sistemos ištekliais valdymas);
- užkarda „bandymams išsisukti“
- ... kiti specialūs uždaviniai

Kriptografijos įrankiai

- be raktų: maišos funkcijos, atsitiktinės bitų sekos, keitiniai;
- su simetriniais raktais: simetriniai šifravimo algoritmai, autentifikavimo kodai, pseudoatsitiktinių bitų srautai;
- su viešuoju raktu: viešo rakto šifravimo algoritmai, parašai...

Kriptosistema – įrankių sistema, naudojama duomenų apsaugai.

Kriptografija ir kriptanalizė

Kriptografija kuria duomenų apsaugos įrankius.

Kriptanalizė bando juos įveikti.

Kriptologija = kriptografija + kriptanalizė

Kriptografiniai protokolai

Kriptografija kuria įrankius informacijos apsaugos uždaviniams spręsti.

Protokolas nurodo, kaip turi elgtis dalyviai, kad pasiektų norimą rezultatą.

Kriptografinis protokolas - protokolas, kuriame naudojami kriptografiniai įrankiai (algoritmai).

Kriptografinių protokolų ypatybė

Protokolų, kurie naudojami kompiuterių tinkluose ypatybė: subjekto, dalyvaujančio protokole tapatybės negalima nustatyti tiesiogiai, t.y. remiantis fizinėmis jo savybėmis.

Veikiantieji asmenys

Algis, Birutė, Justas, Zigmas, ...

Kriptografinės apsaugos atakos

Atakos gali būti nukreiptos

- į kriptografinius algoritmus
- į algoritmų naudojimo metodus
- į kriptografinius protokolus

Kriptografinių protokolų atakos

Pasyvios (kriptografinių protokolų vykdymo duomenų analizė)

Aktyvios (įsibrovimas į kanalą, duomenų keitimas, apsimetimas...)

Aktyvios kriptografinių protokolų atakos

- Žinomų raktų ataka
- Protokolo kartojimas
- Apsimetimo ataka
- Žodyno ataka
- Įsiterpimo ataka

Prielaidos apie Z

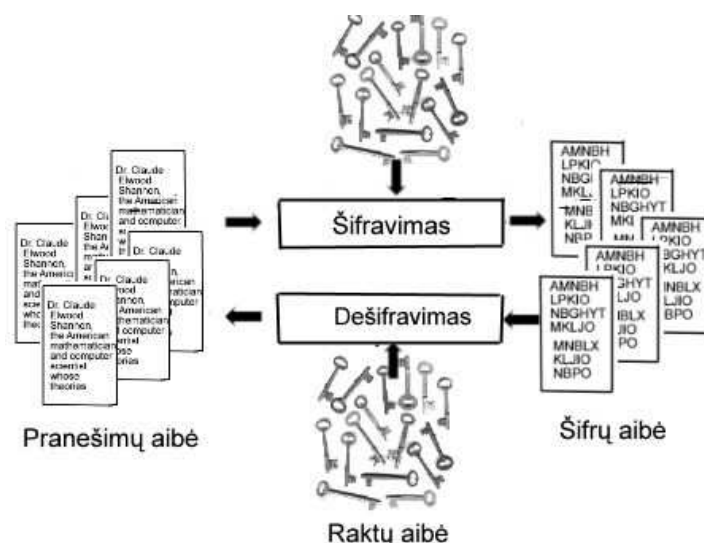
- gali nukopijuoti bet kokius seanso metu siunčiamus duomenis
- gali pakeisti bet kurį pranešimą
- gali pasiųsti seanso pranešimą kitu adresu
- Z gali būti pašalinis asmuo, o taip pat – teisėtas protokolo dalyvis
- gali gauti ankstesnių protokolų slaptus duomenis (raktus)

Kriptografinės duomenų apsaugos įrankiai

- simetrinės kriptosistemos
- viešojo rakto kriptosistemos
- skaitmeniniai parašai
- maišos funkcijos (h-funkcijos)
- autentifikavimo kodai (MAC)
- pseudoatsitiktinių skaičių generatoriai
- ...

Kriptosistema

Duomenų slaptumą užtikrina šifravimas



Kriptosistema

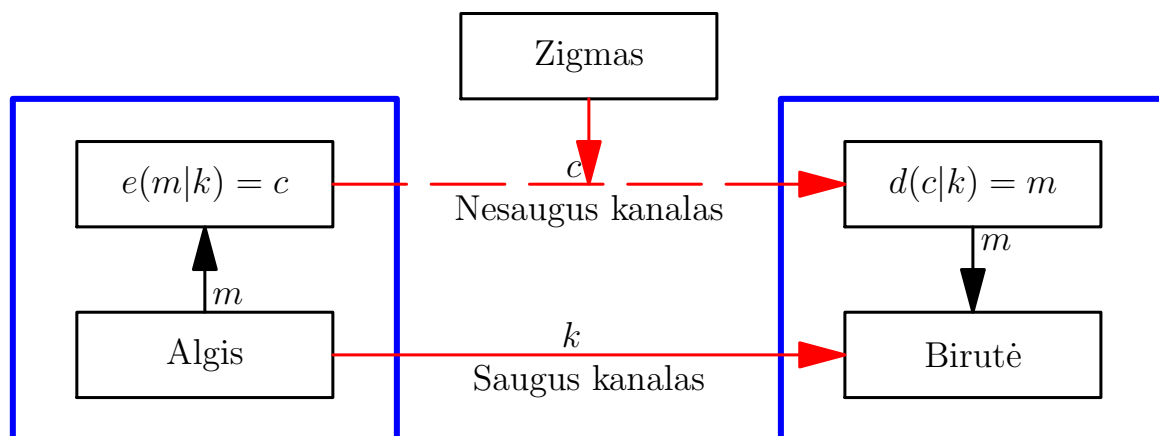
Apibrėžimas. Kriptografinė sistema (kriptosistema) vadinsime aibių trejetą $\langle \mathcal{M}, \mathcal{K}, \mathcal{C} \rangle$ ir atvaizdžių porą

$$e(\cdot|K) : \mathcal{M} \rightarrow \mathcal{C}, \quad d(\cdot|K) : \mathcal{C} \rightarrow \mathcal{M}, \quad K \in \mathcal{K}.$$

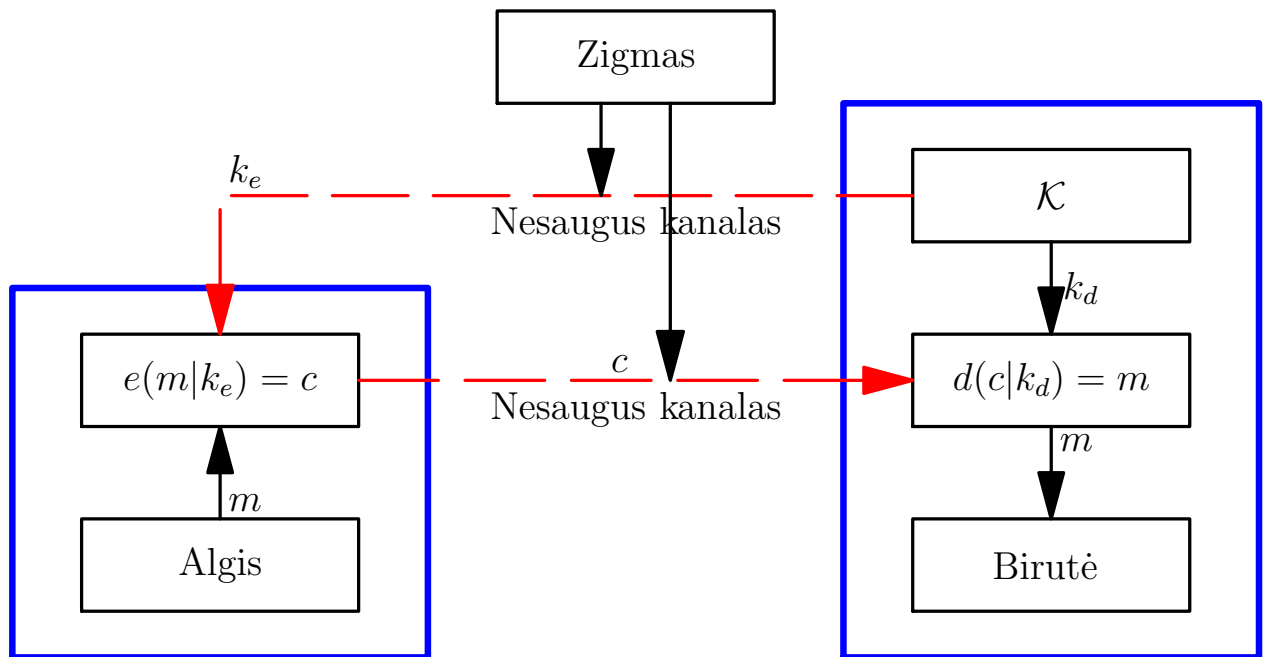
Apie kriptosistemos elementus galvojame taip:

- \mathcal{M} – pranešimų, kuriuos galima šifruoti, aibė;
- \mathcal{K} – raktų, kuriuos galima naudoti, aibė;
- \mathcal{C} – šifrų aibė;
- $e(\cdot|K)$ – šifravimo algoritmas, kurį valdo raktas K ;
- $d(\cdot|K)$ – dešifravimo algoritmas, kurį valdo raktas K ,

Simetrinės kriptosistemos

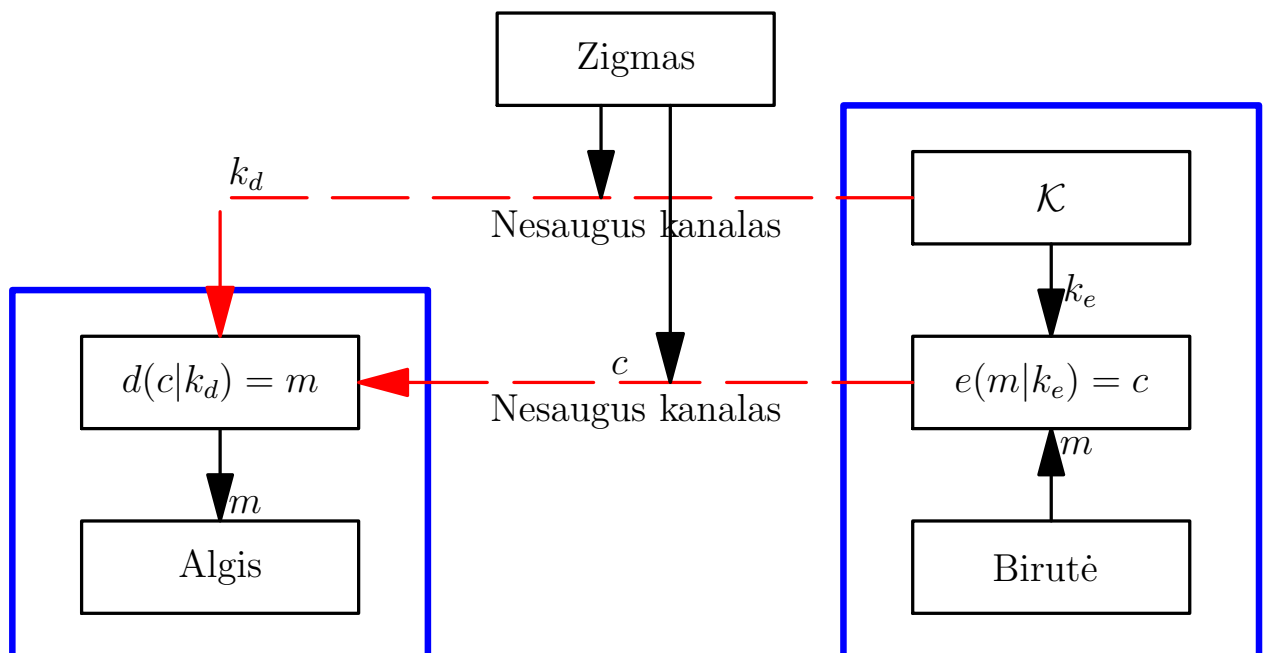


Nesimetrinės kriptosistemos

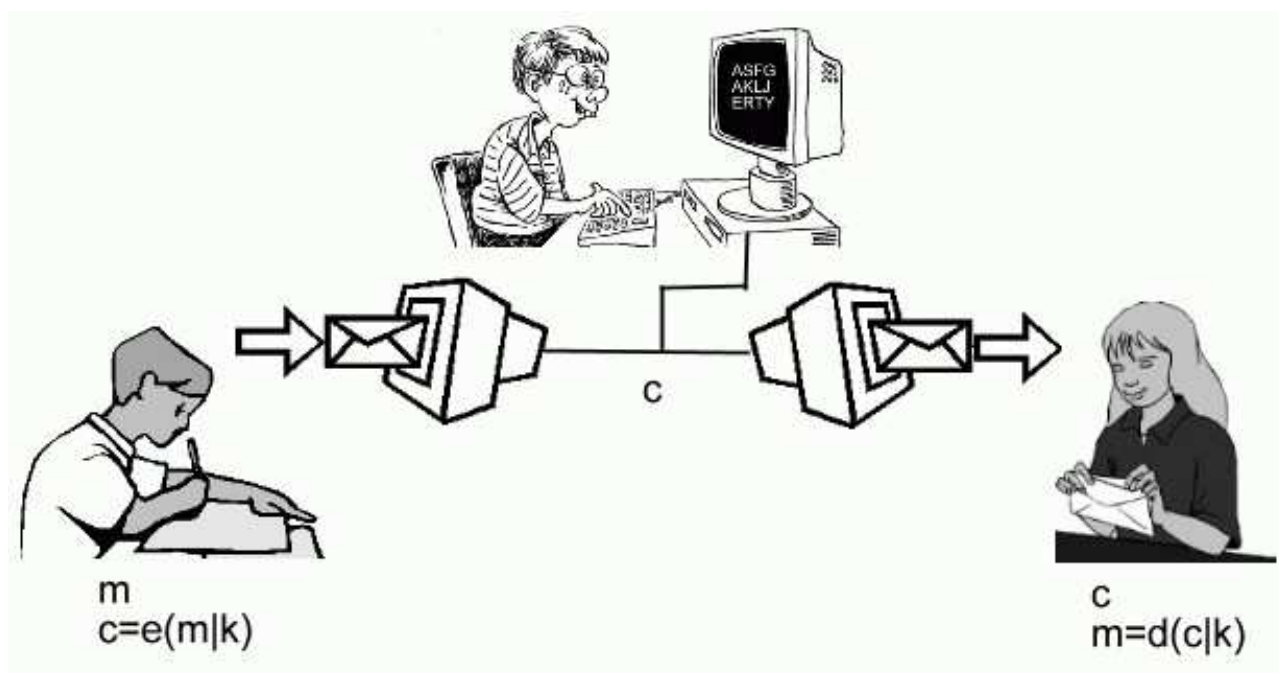


Skaitmeniniai parašai

Pranešimo autentiškumo užtikrinimo įrankis – skaitmeninis parašas



Atakos



Tikslas: naudojantis turima informacija apie kriptosistemą įgyti galimybę dešifruoti šifrus.

Kerckhoffo aksioma

Priešininkas žino apie kriptosistemą viską, išskyrus raktą.

Atakų rūšys:

- kriptosistemų struktūros atakos
- kriptosistemų realizacijos (kanalų) atakos
- protokolų atakos

Kriptosistemų struktūros atakos

Tikslas: surasti raktą arba efektyvų būdą dešifruoti be rakto.

- pavienių šifrų ataka;
- teksto-šifro porų ataka;
- pasirinktų teksto-šifro porų ataka;
- adaptivi pasirinktų teksto-šifro porų ataka;
- pasirinktų šifrų ataka.

Kriptosistemų saugumo vertinimas

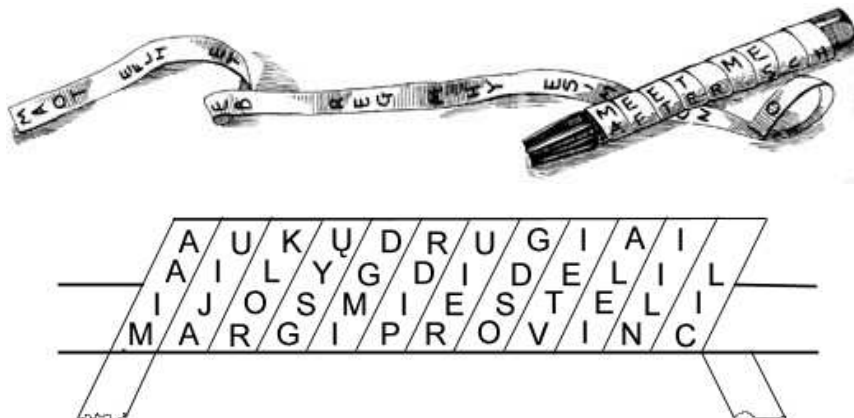
- besąlygiškas saugumas;
- saugumas sudėtingumo teorijos požiūriu;
- saugumas skaičiavimų išteklių požiūriu;
- įrodytas saugumas;
- ad hoc saugumas.

2. Klasikinė kriptografija

Perstatų šifrai

Informacijos struktūra paslepiama perstatant simbolius.
Kaip užrašyti perstatų šifro rakta?

Skytalės šifras



Skytalė: šie tiek Sage kodo

```
abc=unicode('AaĄąBbC...RrSsŠšTtUuŲųŪūVvZzŽž','utf-8')
abcD=unicode('AĄBCČDEĘĖFGHIĮYJKLMNOPRSŠTUŲŪVZŽ','utf-8')
```

```
def pertv(text): # Pašalina ne abėcėlės ženklus
    textn=''
    for a in text:
        if a in abc:
            textn+=a
    return textn.upper()
```

```
tx=unicode('aa22čččč sssddūūū','utf-8')
print pertv(tx)
```

AAČČČČSSSDDŪŪŪ

Skytalė: šie tiek Sage kodo

```
def skytale(text,key):
    textn=pertv(text)
    c=''
    ilg=len(text)
    r=key-ilg%key
    if r<key:
        textn+=textn[0:r]
    ilg=len(textn)
    eil=ilg//key
    for i in range(0,eil):
        for j in range(0,key):
            c+=textn[i+j*eil]
    return c
```

```
tekstas=unicode('žvarbus vėjas pūtė visą dieną','utf-8')
print skytale(tekstas,4)
```

ŽVTIVĖĖĖAJVNRAIABSSŽUPAVSŪDA

Perstatų šifras

P	R	I	S	I	P	A	Ž	I	N
O	J	O	N	A	V	A	Š	I	L
U	T	E	I	L	A	B	A	I	K
A	U	N	U	Ž	I	N	O	K	I
T	N	O	R	I	S	B	Ū	T	I
T	U	R	I	U	G	A	M	Y	K
L	Ą	P	U	I	K	I	Ą	I	L
G	Ą	K	A	M	I	N	Ą	U	Ž
T	E	R	Š	T	T	I	K	R	A
I	P	A	J	È	G	Č	I	A	U
J	Ū	S	Ų	N	E	M	U	N	Ą

Raktas: SAULĖTEKIS → 7-1-10-6-3-9-2-5-4-8 **Perstatų šifras**

Perstatų šifrus sunku įveikti!

VESINTNVONMWSFEWNOEALWRNRNCFITEEICRHCODEEA
HEACAEOHMYTONTDFIFMDANGTDRVAONRRTORMTDHE
OUALTHNFHHWHLESLIIAOETOUTOSCDNRITYEELSOANGP
VSHLRMUGTNUITASETNENASNANRTTRHGUODAAARAO
EGHEESAODWIDEHUNNTFMUSISCDLEDTRNARTMOOIREEY
EIMINFELORWETDANEUTHEEEENENTHEOOEAUEAEAHUHI
CNCGDTUROUTNAEYLOEINRDHEENMEIAHREEDOLNNIRAR
PNVEAHEOAATGEFITWMYSOTHTHAANIUPTADLRSRSDNOT
GEOSRLAAURPEETARMFEHIREAQEEOILSEHERAHAOTNT
RDEDRSDOOEGAEFPUOBENADRNL EIAFRHSASHSNAMRLT
UNNTPHIOERNESRHAMHIGTAETOHSENGFTRUANIPARTAOR
SIHOOAEUTRMERETIDALSDIRUAIEFHRHADRESEDNDOION
ITDRSTIEIRHARARRSETOIHOKETHRSRUAODTSCTTAFSTHCA
HTSYAOLONDNDWORIWHLNTHMHMTLCVROSTXVDRESDR

1999 metais vokiečių kriptologo O. Leibericho sudarytas dvigubų perstatų šifras. Neiišifruotas iki šiol!

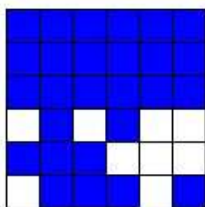
Geležinkelio tvorelės šifras

Ž T I N M S T
 E E Ū R N I T E E Ū L N A
 M I S A I R A Ž M N A I I
 E L V S A K O O P I B R
 J A I P A I

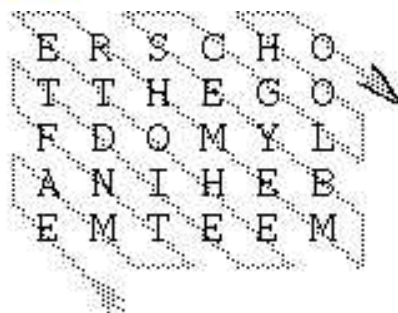
Rail-fence

„Geometrinės“ perstatos

Kapitono Fleisnerio
kvadratas



E R S C H O
 T T H E G O
 F D G M Y L
 A N I H E B
 E M T E E M



Fleisner

Keitinių šifrai

\mathcal{A}, \mathcal{B} – teksto ir šifro abėcėlės,

$$e(\cdot|K) : \mathcal{A} \rightarrow \mathcal{B}$$

injektyvus atvaizdis,

$$e(m_1 m_2 \dots m_n | K) = e(m_1 | K) e(m_2 | K) \dots e(m_n | K)$$

Polibijaus kodas

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

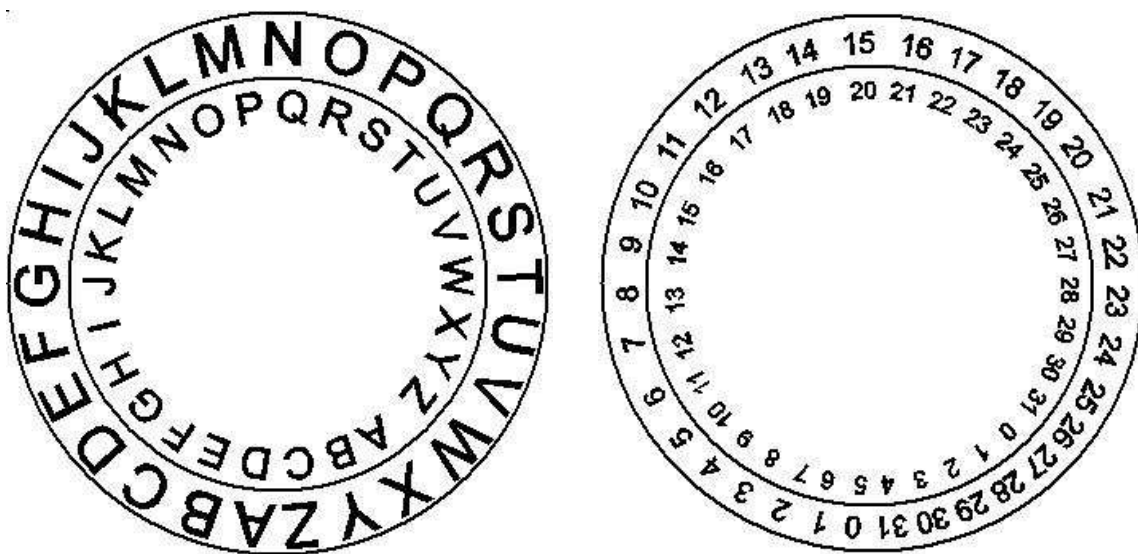
Polibijaus kodas

Polibijaus kodo variacijos

Dellastelio šifras (1895)

Hayhaneno šifras (1953)

Cezario šifras



Cezario šifras

$$\mathcal{A} = \mathcal{B} = \mathcal{K} = \{0, 1, 2, \dots, n-1\}$$

$$e(a|k) = a + k \pmod{n}$$

Didesnė Cezario šifrų klasė:

$$\mathcal{A} = \mathcal{B} = \{0, 1, 2, \dots, n-1\},$$

$$\mathcal{K} = \{\langle k_1, k_2 \rangle : (k_1, n) = 1\}$$

$$e(a|k_1, k_2) = k_1 a + k_2 \pmod{n}$$

Playfairio (Wheatstono) šifras



P	L	A	Y	F	P	L	A	Y	F
I	R	E	X	M	I	R	E	X	M
B	C	D	G	H	B	C	D	G	H
K	N	O	Q	S	K	N	O	Q	S
T	U	V	W	Z	T	U	V	W	Z

Variacijos: trijų kvadratų šifras

Hilo šifras

$$\mathcal{A} = \mathcal{B} = \{\langle i, j \rangle : 0 \leq i, j < n\},$$

$$\mathcal{K} = \left\{ K : K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}, 0 \leq k_{ij} < n, (\det(K), n) = 1 \right\}$$

$$e(\langle m_1, m_2 \rangle | K) = \langle m_1, m_2 \rangle \cdot K \pmod{n}$$

Galima šifruoti ne tik poras, bet ir ilgesnes sekas.

Homofonai

Chiffre de SULLY (1599)

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	X	Y	Z
3	20	8	11	7	2	15	4	12	16	1	13	17	5	19	14	18	6	9	22	21	10
J	f	g	h	i	k	l	m	n	p	q	r	s	t	u	v	w	x	y	z	a	b
c	d	e	f	g	h	i	k	l	m	n	p	q	r	s	t	u	v	w	x	y	z

le Roy	4	ayant	a	il	9
le Pape	3	ans	b	le	8
le Roy d'Espagne	2	argent	c	la	7
l'Empereur	5	actendu	d	lettre	6
le Grand Seigneur	6	actendant	e	mois	5
la Roynie d'Angleterre	7	sprès	f	ment	4
le Roy d'Ecosse	8	buy	g	mons	3
l'Archiduc d'Autriche	9	bon	h	nous	2
l'Infante d'Espagne	10	beau	j	nostre	1
les Etats des Pays-Bas	11	bailli	k	nest	0
la Seigneurie de Venise	12	car	l	non	9
le Roy du Danemark	13	convient	m	ouverture	8
le Roy de Subde	14	cen	n	occasion	7
les Cantons Suisses	15	contenant	o	oultre	6



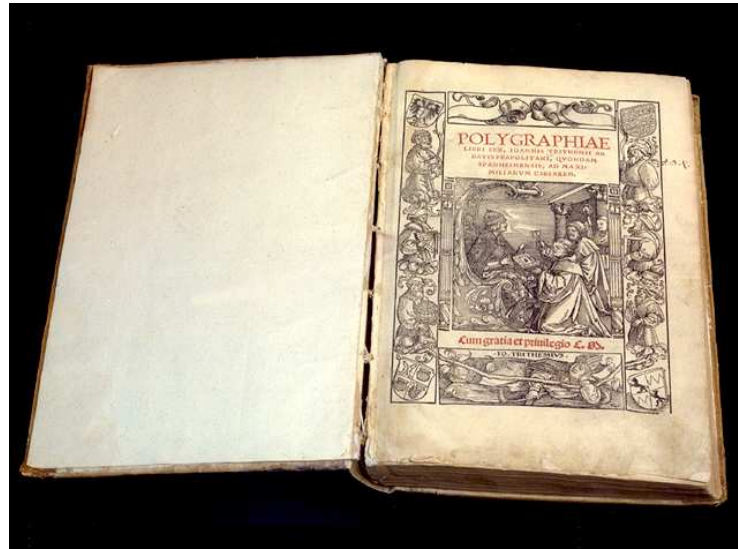
Homofonai iš teksto

De la Porta homofonų šifras

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	Z	
♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	♀	A
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	B
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	C
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	D
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	E
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	F
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	G
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	H
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	I
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	L
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	M
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	N
♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	♀	♂	O
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	P
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	Q
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	R
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	S
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	T
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	V
♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	Z

2.3 Šifrai su daugeliu abėcėlių

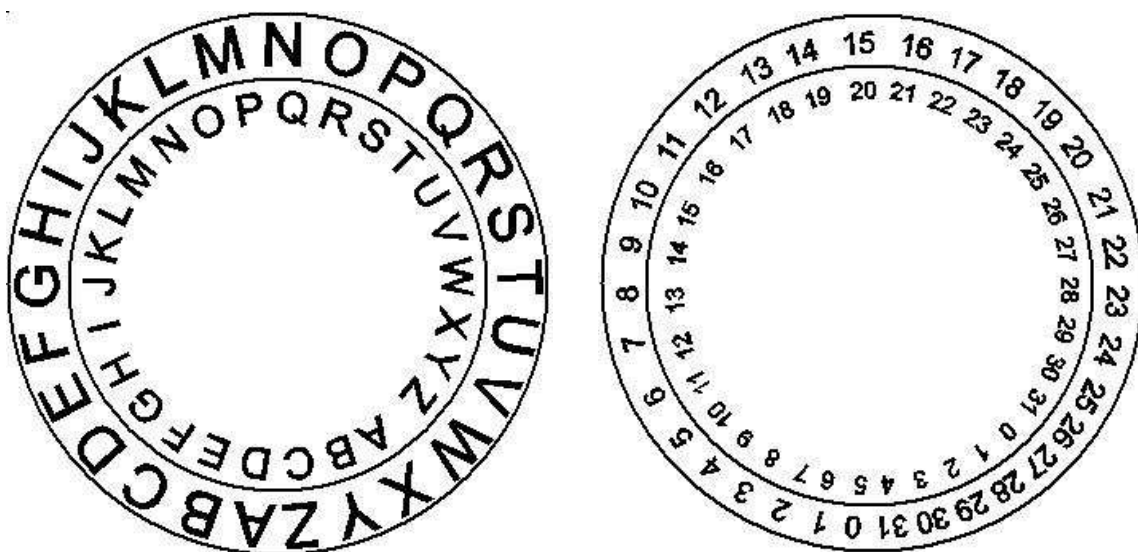
Johannes Trithemius (1462 – 1516)



Tabula recta

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A			
A	B	C	D	E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	
B	C	D	E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	
C	D	E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	
C	D	E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C
D	E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D
E	E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E
E	F	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E
F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G
G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H
H	I	J	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H
I	J	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I
I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J
J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K
K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L
L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M
L	M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M
M	N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
N	O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O
O	P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P
P	R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R
R	S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S
S	S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S
S	T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T
T	U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U
U	U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	V
U	V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	V	Z
V	Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z
Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A
Z	A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	S	T	U	U	V	Z	A

Alberti skrituliai, Vigenere šifras



Vigenere šifras

$$\mathcal{A} = \{0, 1, \dots, n-1\}$$

$$\begin{array}{rcl} M & = & m_1 \quad m_2 \quad \dots \quad m_d \quad m_{d+1} \quad m_{d+2} \quad \dots \quad m_{2d} \\ K & = & k_1 \quad k_2 \quad \dots \quad k_d \quad k_1 \quad k_2 \quad \dots \quad k_d \\ M & = & c_1 \quad c_2 \quad \dots \quad c_d \quad c_{d+1} \quad c_{d+2} \quad \dots \quad c_{2d} \end{array}$$

$$c_{j+td} = m_{j+td} + k_j \pmod{n}$$

Vigenere šifras

Vigenere šifro analizė

Jei žinotume rakto ilgį d

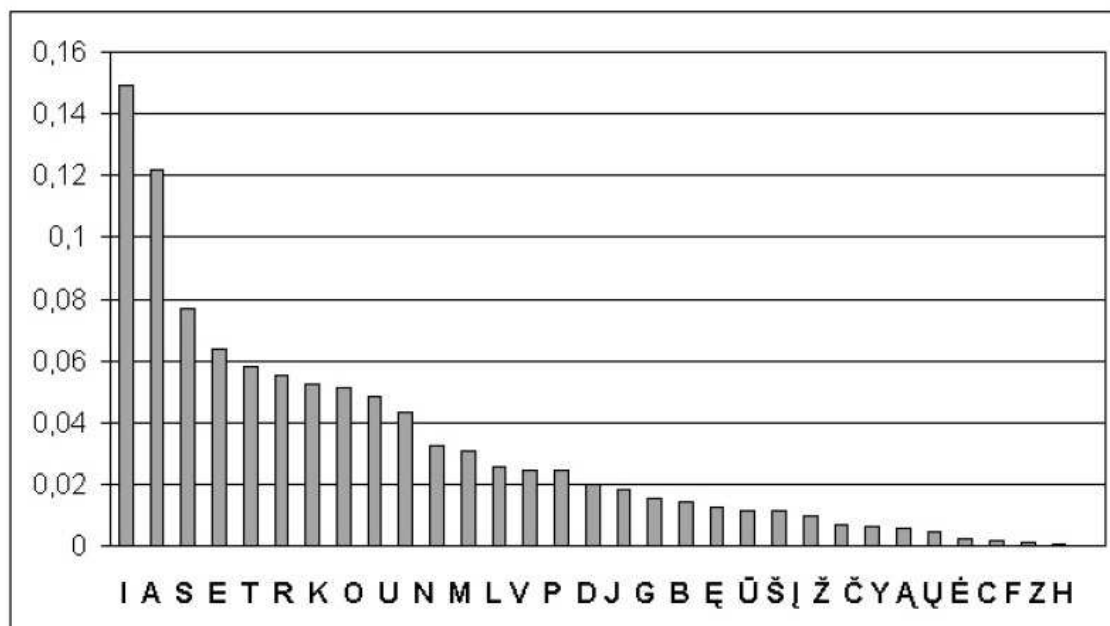
$$\begin{array}{llll} M_1 & = & m_1 m_{1+d} m_{1+2d} \dots m_{1+td} \dots & \rightarrow C_1 = c_1 c_{1+d} c_{1+2d} \dots c_{1+td} \dots \\ M_2 & = & m_2 m_{2+d} m_{2+2d} \dots m_{2+td} \dots & \rightarrow C_2 = c_2 c_{2+d} c_{2+2d} \dots c_{2+td} \dots \\ \vdots & & \vdots & \vdots \\ M_d & = & m_d m_{2d} m_{3d} \dots m_{td} \dots & \rightarrow C_d = c_d c_{2d} c_{3d} \dots c_{td} \dots \end{array}$$

Kassiskio testas

PAVARGĖS VASARIS PUSNYNUOSE MIEGA IR VANDENYS SLŪGSO UŽŠALĘ
LAUKASLA UKASLAU KASLAUKASL AUKAS LA UKASLAUK ASLAUK ASLAUK

Kassiskio testas

Lietuvių kalbos dažniai



Sutapimų indeksas

$$\kappa = p_0^2 + p_1^2 + \dots + p_{n-1}^2$$

Lietuvių kalbos sutapimų indeksas

$$\kappa_{\text{liet}} = p_0^2 + p_1^2 + \dots + p_{31}^2 \approx 0,069$$

Friedmano testas

Kiek vienodų stulpelių lentelėse

$$\begin{vmatrix} c_1 & c_2 & c_3 & \dots \\ c_2 & c_3 & c_4 & \dots \end{vmatrix} \quad \begin{vmatrix} c_1 & c_2 & c_3 & \dots \\ c_3 & c_4 & c_5 & \dots \end{vmatrix} \dots \begin{vmatrix} c_1 & c_2 & c_3 & \dots \\ c_j & c_{j+1} & c_{j+2} & \dots \end{vmatrix}$$

Testai

Friedmano rakto ilgio formulė

Teksto ir šifro abėcėlė $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$

Raidžių a_i tikimybės nešifruotame tekste p_i yra žinomos, Vigenere šifre q_i yra nežinomos, tačiau turint ilgą šifrą galima skaičiuoti raidžių dažnius.

Sutapimų indeksai

$$I_M = \sum_{i=1}^n p_i^2, \quad I_M = \sum_{i=1}^n q_i^2, \quad I_0 = \sum_{i=1}^n \frac{1}{n^2}$$

Friedmano rakto ilgio formulė

Žinomas ilgas Vigenere šifras $C = c_1 c_2 \dots c_N$ norime sužinoti rakto ilgį d . Jei d žinotume, galėtume sudaryti lentelę

$$\begin{array}{cccc} c_1 & c_{1+d} & c_{1+2d} & \dots \\ c_2 & c_{2+d} & c_{2+2d} & \dots \\ \vdots & \vdots & \vdots & \vdots \\ c_d & c_{2d} & c_{3d} & \dots \end{array}$$

Kiekviena eilutė – Cezario šifras, jame $\approx N/d$ raidžių.

Friedmano rakto ilgio formulė

$$\begin{array}{cccc} c_1 & c_{1+d} & c_{1+2d} & \dots \\ c_2 & c_{2+d} & c_{2+2d} & \dots \\ \vdots & \vdots & \vdots & \vdots \\ c_d & c_{2d} & c_{3d} & \dots \end{array}$$

Atsitiktinai renkame dvi šifro raides x, y .
Skaičiuosime tikimybę $P(x = y) = I_C$:

$$P(x = y) = P(x = y|A)P(A) + P(x = y|\bar{A})P(\bar{A})$$

Friedmano rakto ilgio formulė

$$\begin{array}{cccc} c_1 & c_{1+d} & c_{1+2d} & \dots \\ c_2 & c_{2+d} & c_{2+2d} & \dots \\ \vdots & \vdots & \vdots & \vdots \\ c_d & c_{2d} & c_{3d} & \dots \end{array}$$

$$I_C = P(x = y) = P(x = y|A)P(A) + P(x = y|\bar{A})P(\bar{A})$$

$$P(x = y|A) = I_M, \quad P(x = y|\bar{A}) = I_0$$

$$P(A) = \frac{N}{2} \left(\frac{N}{d} - 1 \right) / C_N^2, \quad P(\bar{A}) = \frac{N}{2} \left(N - \frac{N}{d} \right) / C_N^2$$

Friedmano rakto ilgio formulė

$$I_C = P(x = y|A)P(A) + P(x = y|\bar{A})P(\bar{A})$$

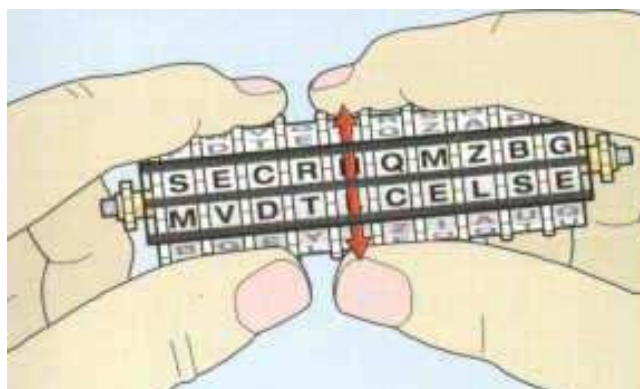
$$I_C = I_M \frac{N}{2} \left(\frac{N}{d} - 1 \right) / C_N^2 + I_0 \frac{N}{2} \left(N - \frac{N}{d} \right) / C_N^2$$

$$d \approx = \frac{N(I_M - I_0)}{I_C(N - 1) + I_M - NI_0}$$

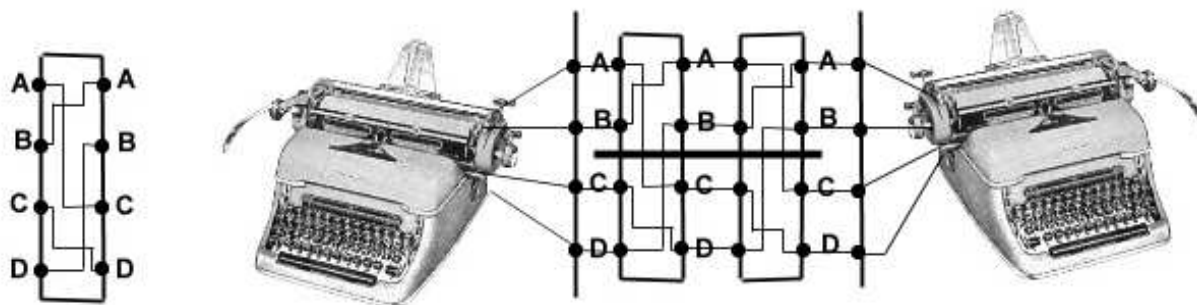
I_C galime apskaičiuoti naudodamiesi raidžių dažniais šifre.

Mechaniniai šifravimo prietaisai

Jeffersono cilindrai



Enigma



$$\rho = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \quad \lambda_1 = \lambda_2 = \begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$$

$$\text{Tekstas} = t_0 t_1 t_2 \dots, \quad t_k, \quad k = m_1 + 4m_2 + \dots$$

$$c_k = \rho^{-m_2} \lambda_2 \rho^{m_2} \rho^{-m_1} \lambda_1 \rho^{m_1}(t_k),$$

$$t_k = \rho^{-m_1} \lambda_1^{-1} \rho^{m_1} \rho^{-m_2} \lambda_2^{-1} \rho^{m_2}(c_k)$$

Enigma su dviem rotoriais

$$\mathcal{A} = \{0, 1, \dots, n-1\},$$

$$\rho = \begin{pmatrix} 0 & 1 & \dots & n-1 \\ 1 & 2 & \dots & 0 \end{pmatrix} = [1, 2, 3, \dots, n-1, 0],$$

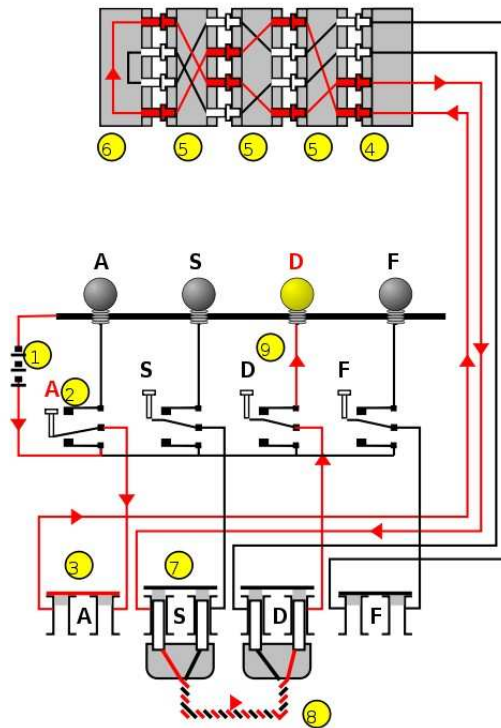
$$\rho^m(a) = a + m \pmod{n}$$

$$\text{Tekstas} = t_0 t_1 t_2 \dots, \quad t_k, \quad k = m_1 + n \cdot m_2 + \dots$$

$$c_k = \rho^{-m_2} \lambda_2 \rho^{m_2} \rho^{-m_1} \lambda_1 \rho^{m_1}(t_k),$$

$$t_k = \rho^{-m_1} \lambda_1^{-1} \rho^{m_1} \rho^{-m_2} \lambda_2^{-1} \rho^{m_2}(c_k)$$

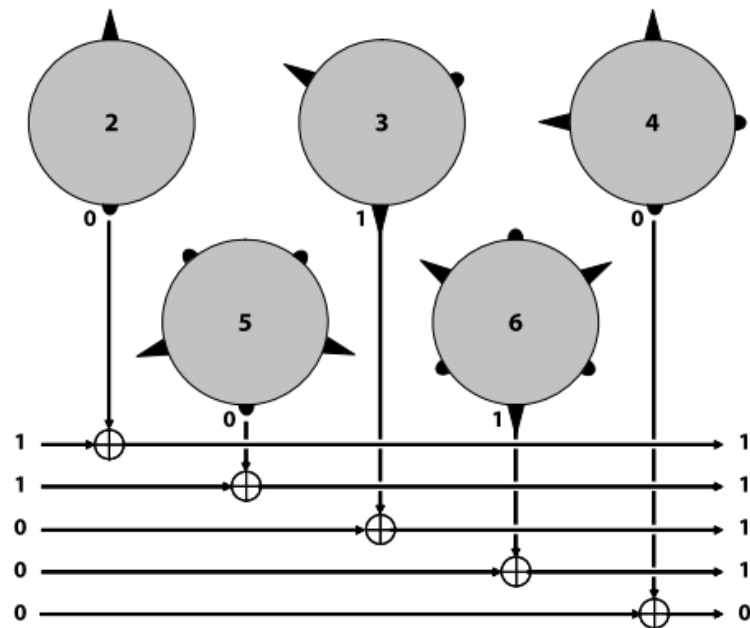
Nesuprastinta ENIGMA



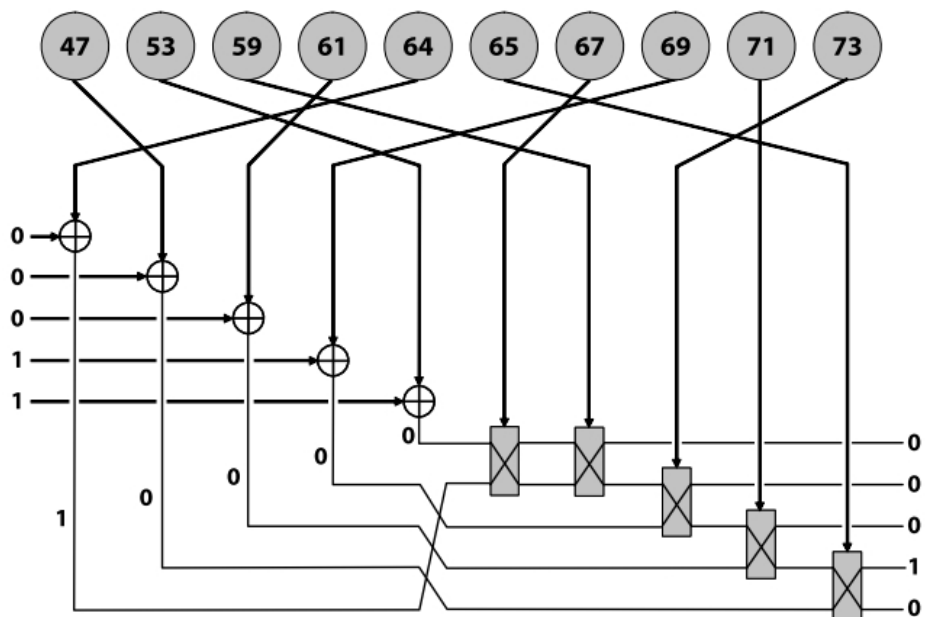
Nesuprastinta ENIGMA

$$\begin{aligned}
 \text{Tekstas} &= t_0 t_1 t_2 \dots, \quad t_k, \\
 k &= m_1 + m_2 \cdot n + m_3 \cdot n^2 + \dots \\
 \alpha(m, \lambda) &= \rho^{-m} \lambda \rho^m, \\
 \alpha^{-1}(m, \lambda) &= \rho^m \lambda^{-1} \rho^{-m} \\
 c_k &= \sigma^{-1} \alpha^{-1}(m_1, \lambda_1) \alpha^{-1}(m_2, \lambda_2) \alpha^{-1}(m_3, \lambda_3) \pi \leftarrow \\
 &\quad \alpha(m_3, \lambda_3) \alpha(m_2, \lambda_2) \alpha(m_1, \lambda_1) \sigma(t_k) \\
 t_k &= \sigma^{-1} \alpha^{-1}(m_1, \lambda_1) \alpha^{-1}(m_2, \lambda_2) \alpha^{-1}(m_3, \lambda_3) \pi^{-1} \leftarrow \\
 &\quad \alpha(m_3, \lambda_3) \alpha(m_2, \lambda_2) \alpha(m_1, \lambda_1) \sigma(c_k)
 \end{aligned}$$

Vokiečių Geheimschreiber



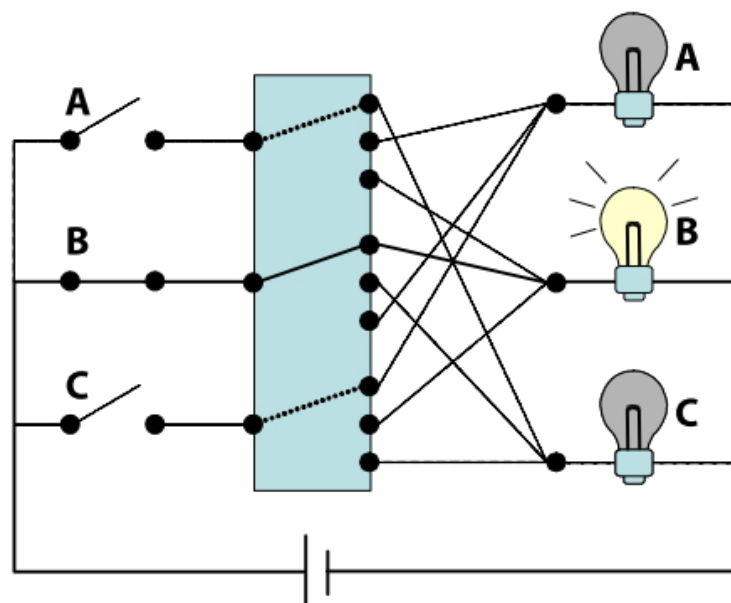
Vokiečių Geheimschreiber



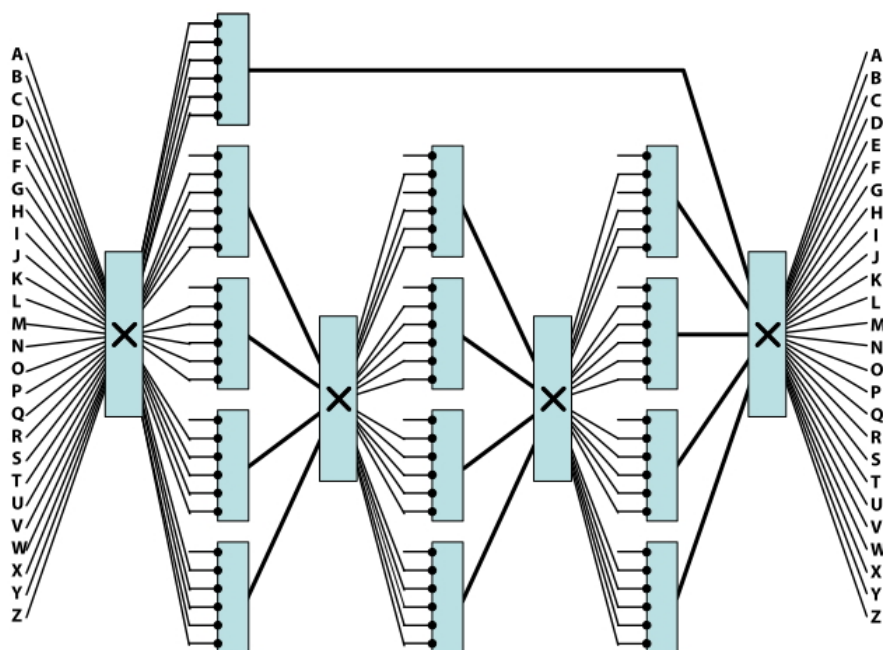
Vokiečių Geheimschreiber



Japonų Purple

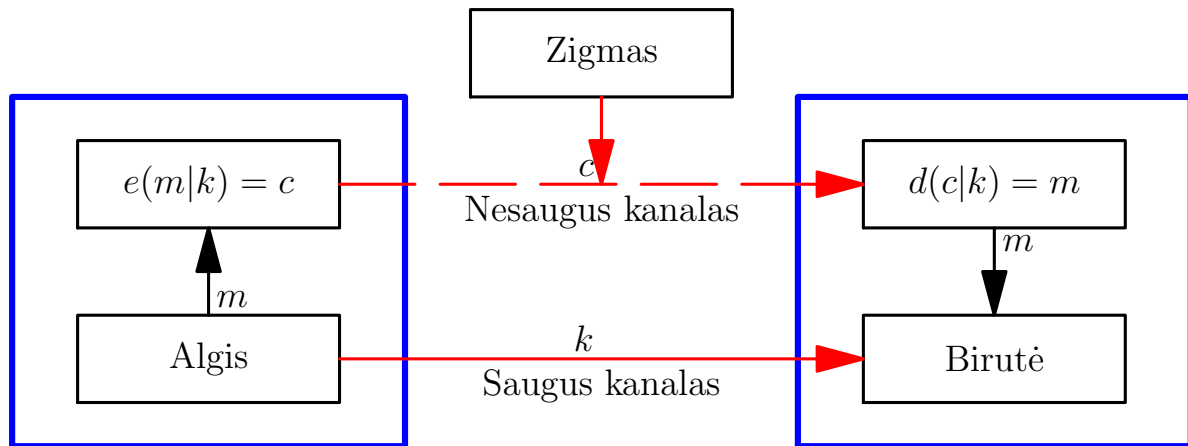


Japonų Purple



2.6 Blokiniai šifrai

Ryšio apsauga simetrine kriptosistema



Pranešimų išraiškos

Unicode Base64

Base64 simboliai – didžiosios ir mažosios lotynų kalbos raidės ir dar du ženklai + ir /.

Koduojamas bitų srautas skaidomas po 6 bitus, gauti blokai verčiami natūraliaisiais skaičiais. Skaičius – raidės sekoje

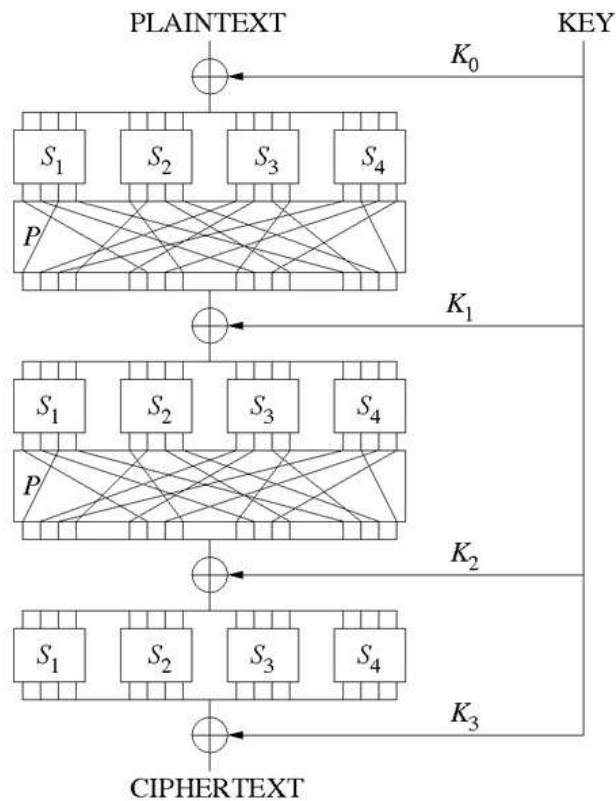
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz0123456789 + /

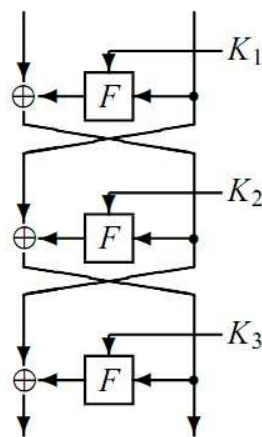
indeksas.

KPT – keitinių-perstatų tinklas

SPN – substitution-permutation network



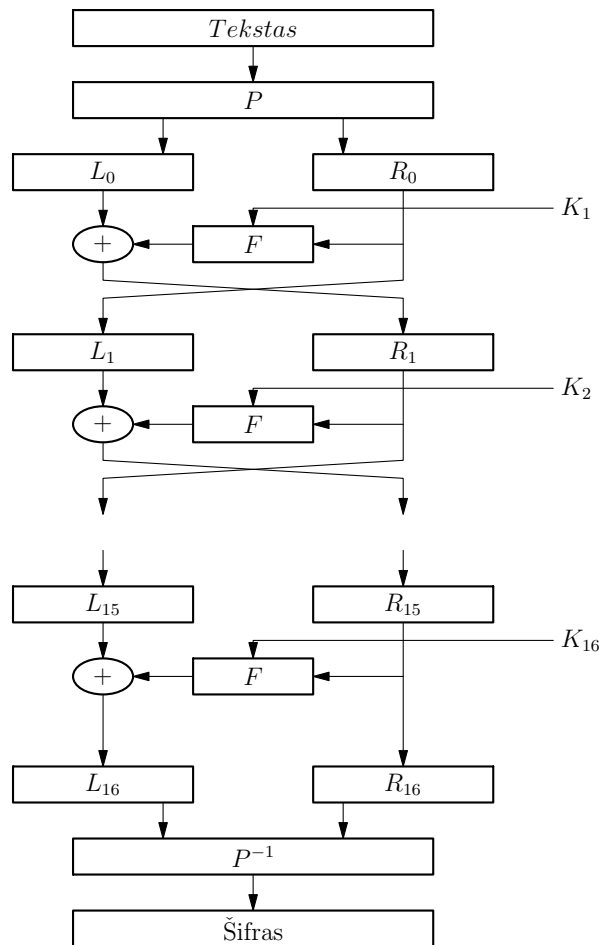
Feistelio schema, DES architektūra



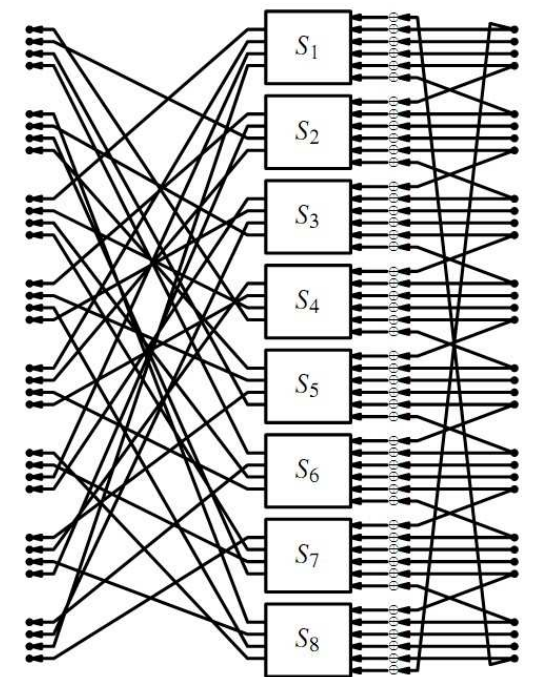
Raktas Kairė (L) Dešinė (R)			Raktas Kairė (L) Dešinė (R)		
K_1	L_0	R_0	K_3	R_3	R_2
K_2	R_0	R_1	K_2	R_2	R_1
K_3	R_1	R_2	K_1	R_1	R_0
	R_2	R_3		R_0	L_0
$C =$	R_3	R_2	$M =$	L_0	R_0

$$R_m = R_{m-2} \oplus F(K_m, R_{m-1}), R_{-1} = L_0$$

DES



Viena DES iteracija



DES dėžės

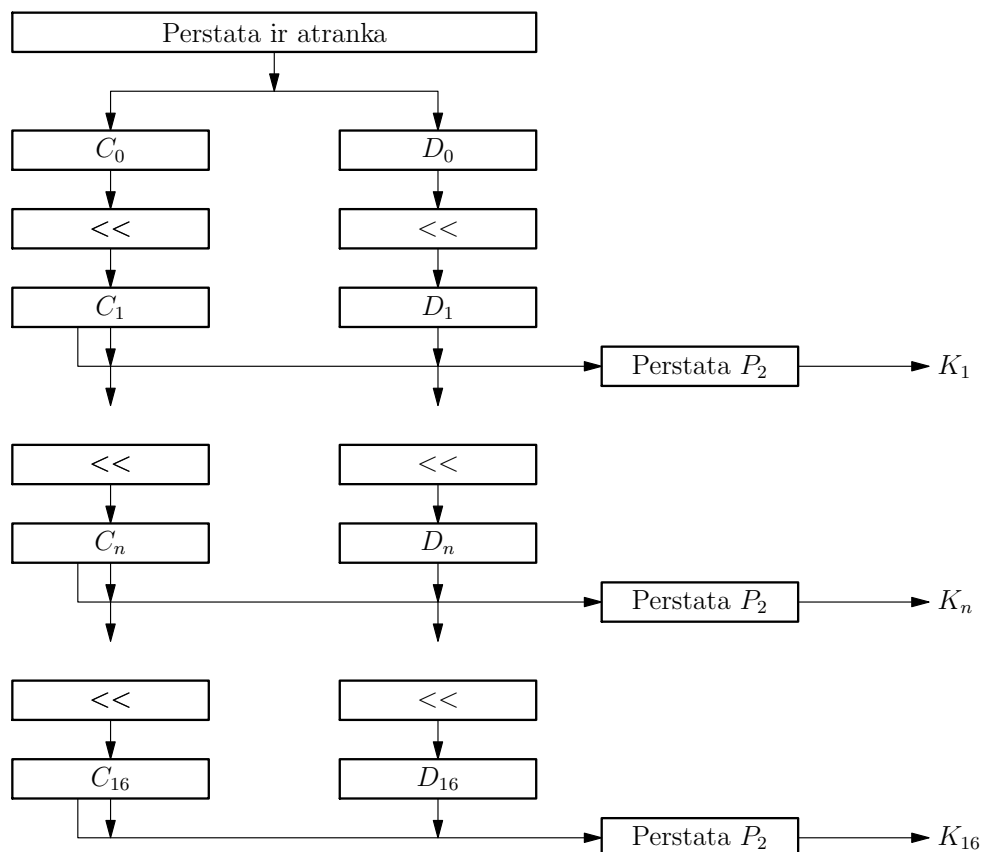
S_I

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES raktai



DES raktai: perstatos

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Postūmių dydžiai

1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

Griūties efektas, kai keičiasi tekstas

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbcb	32
8	67117cf2c11bfc09 2b2cefbcb99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bcla8d9	29
14	c6a62c4e56b0bd75 4bcla8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP⁻¹	da02ce3a89ecac3b 057cde97d7683f2a	32

Griūties efektas, kai keičiasi raktas

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeaaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP ⁻¹	da02ce3a89ecac3b ee92b50606b62b0b	30

DES kriptanalizė

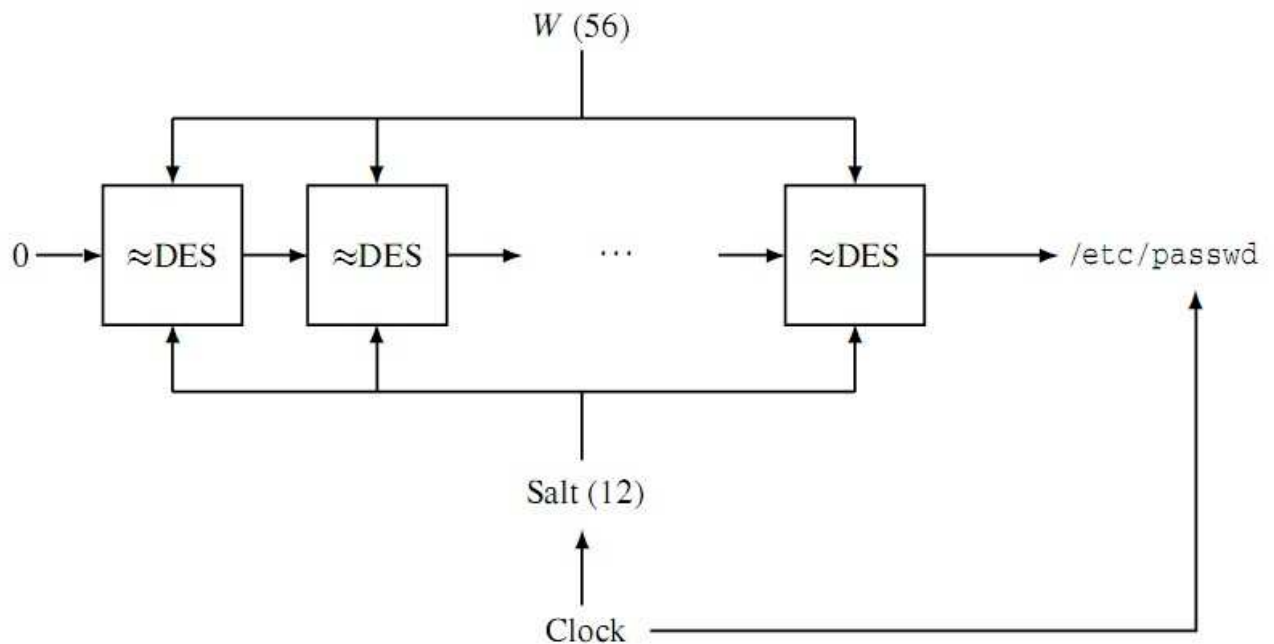
Diferencialinės (skirtuminės) kriptanalizės metodas paskelbtas apie 1990 metus.

Turint 2^{47} pasirinktų teksto-šifro porų galima nustatyti DES raktą atlikus apie 2^{47} operacijų.

Tiesinė kriptanalizė (apie 1993 metus).

Turint 2^{43} pasirinktų teksto-šifro porų galima nustatyti DES raktą atlikus apie 2^{43} operacijų.

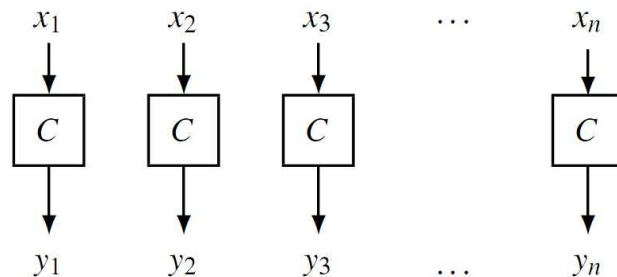
UNIX slaptažodžiai ir DES



Slaptažodžių saugojimas su „druska“

Slaptažodis	Druska	Saugoma
<i>nutmeg</i>	<i>Mi</i>	<i>MiqkFWCm1fNJI</i>
<i>ellen1</i>	<i>ri</i>	<i>ri79KNd7V6.Sk</i>
<i>Sharon</i>	<i>./</i>	<i>./2aN7ysff3qM</i>
<i>norahs</i>	<i>am</i>	<i>amfIADT2iqjAf</i>

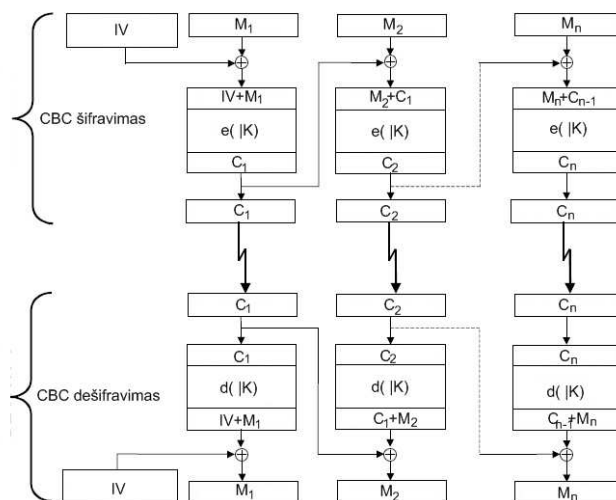
EBC režimas



Blokai gali būti pašalinti, pakeisti, sukeisti... Tas pats blokas visada šifruojamas vienodai.

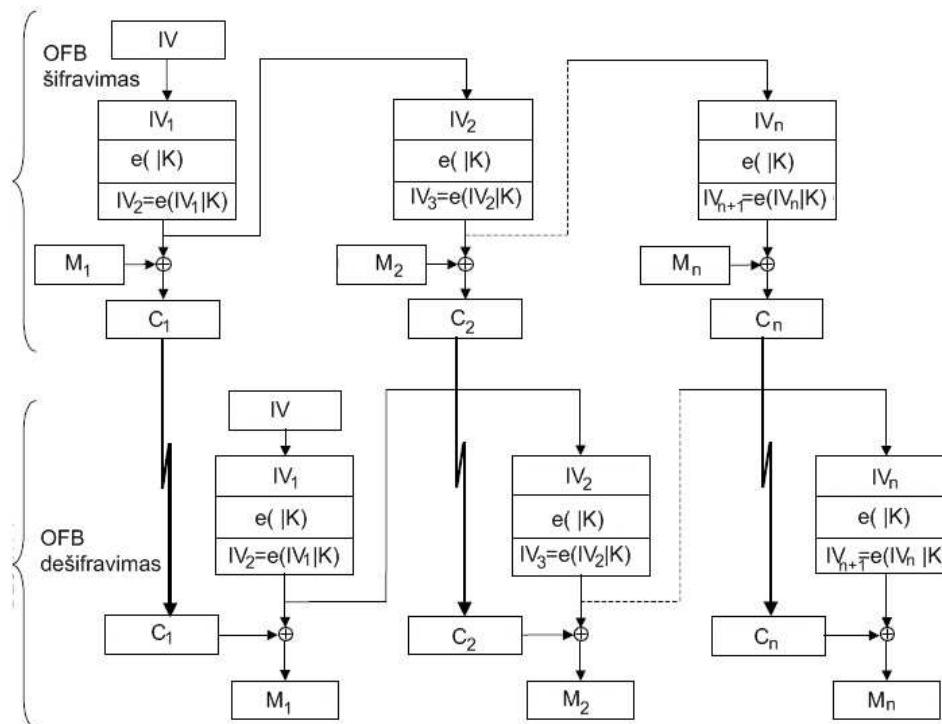
Šifrų blokų grandinės režimas (CBC)

$$C_1 = e(M_1 \oplus IV | K), C_i = e(M_i \oplus C_{i-1} | K), i \geq 2,$$
$$M_1 = d(C_1 \oplus K | IV), M_i = e(C_i | K) \oplus C_{i-1}, i \geq 2.$$

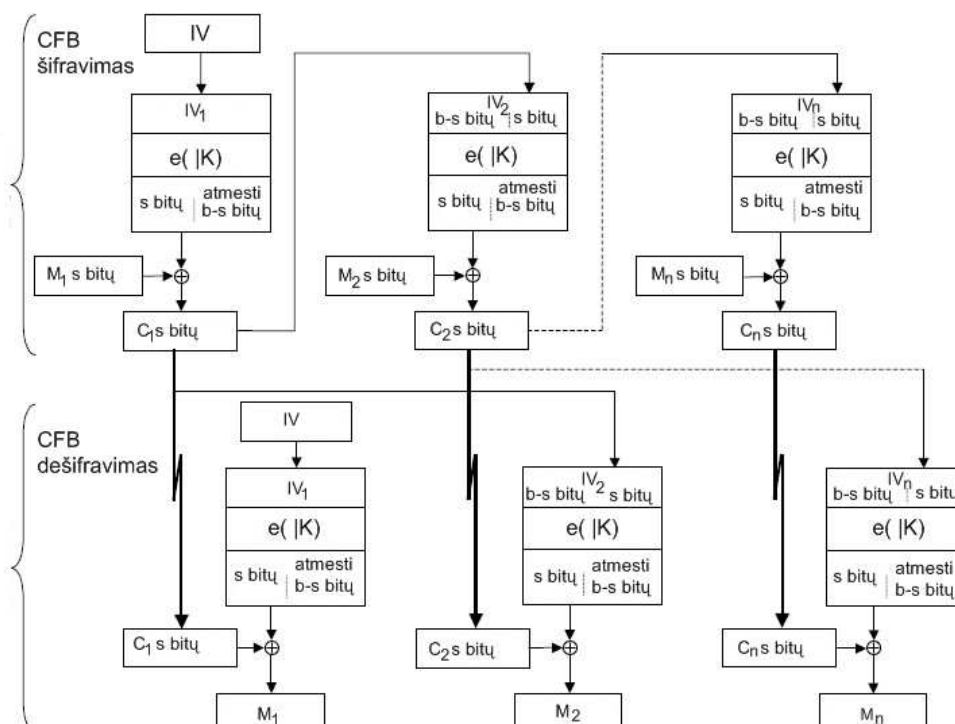


IV nebūtinai slaptas. Kelis šifro blokus pakeitus, kiti blokai bus iššifruojami gerai.

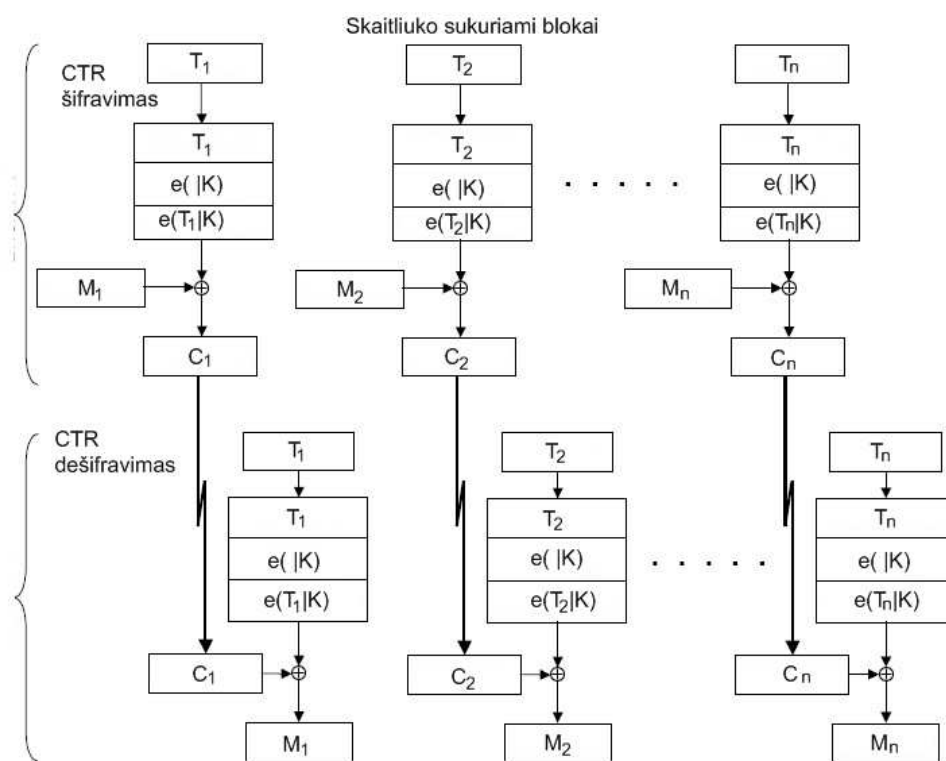
Srauto atgalinio ryšio režimas (OFB)



Šifro atgalinio ryšio režimas (CFB)



Skaitliuko režimas (CTR)



Trigubas DES

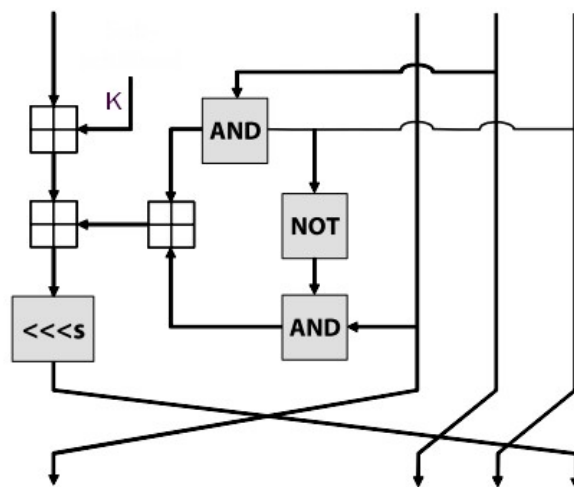
DES: $M \mapsto C = e(M|K), M \in \mathcal{B}^{64}, K \in \mathcal{B}^{56}, \mathcal{B} = \{0, 1\}.$

Trigubas DES: $M \mapsto C = e(d(e(M|K_1)|K_2)|K_3), M \in \mathcal{B}^{64}, K_i \in \mathcal{B}^{56}.$

DES chronologija

1973-05-15	NBS paskelbė kriptostandarto konkursą
1974-08-27	Pakartotinas konkurso skelbimas
1975-03-17	DES paskelbta aptarimui ir kritikai
1976-08	Pirmoji DES konferencija
1976-09	Antroji DES konferencija
1976-11	DES patvirtinta standartu
1977-01-11	Paskelbtas DES standartas FIPS PUB 46
1983	DES pakartotinai patvirtinta standartu
1988-01-22	DES pakartotinai patvirtinta standartu
1992	Teorinė DES ataka (Bihamo ir Shamiro skirtuminė kriptanalizė)
1993-12-30	DES pakartotinai patvirtinta standartu
1994	Eksperimentinė DES ataka (Matsui tiesinė kriptanalizė)
1998	Kompiuteris Deep Crack rado DES raktą per 56 valandas
1999-01	Deep Crack ir lygiagrečių skaičiavimų tinklas ataka – 22 val. 15 min.
1999-10-25	DES pakartotinai patvirtinta standartu – triguba DES
2001-11-26	Paskelbtas AES
2002-05-24	AES įsigaliojo
2004-07-26	DES standartas atšauktas

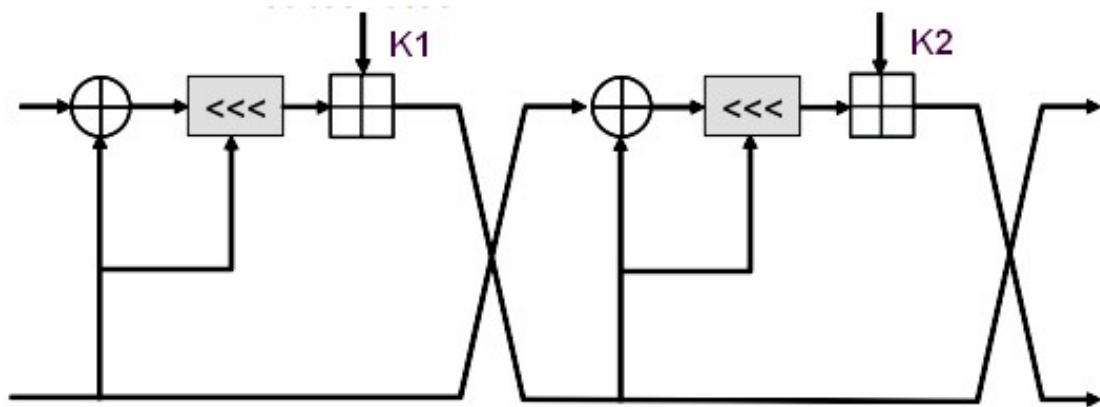
RC2 (Rivest Cipher)



Pranešimo blokas 64 bitai = 4×16

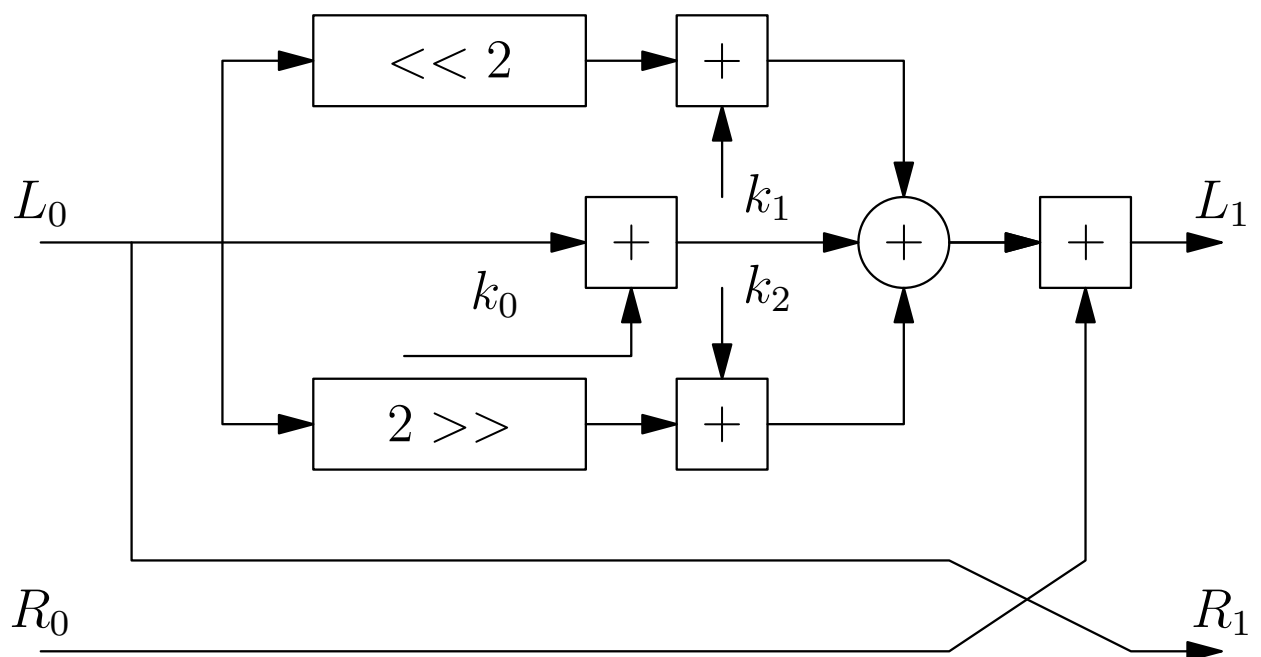
Raktai K_0, K_1, \dots, K_{63} . Sudėčiai su pranešimo bloku naudojamas raktas K_m , m nusako dešiniojo kaimyninio bloko 6 paskutiniai bitai

RC5 (Rivest Cipher)

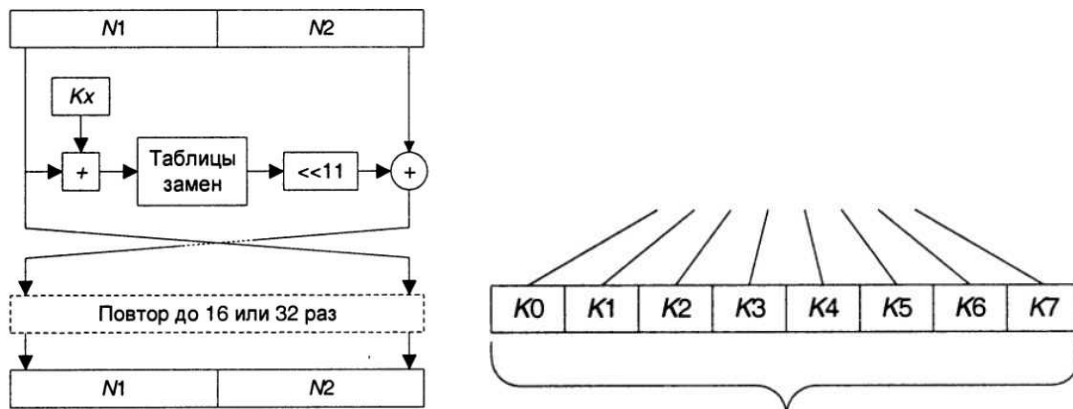


Pranešimų blokai 32, 64, 128 bitų ilgio

TEA (Tiny Encryption Algorithm)



Kiti blokiniai šifrai: GOST 28147-89



64 bitų blokai, 256 bitų ilgio raktas

AES konkursas

1997 JAV Nacionalinis standartų ir technologijų institutas (NIST – National Institute of Standards and Technology) paskelbė naują konkursą garbingojo DES vietai užimti. Atsirado 15 kandidatų. Į finalą išėjo šie: MARS, RC6, Rijndael, Serpent ir Twofish. Nugalėjo Rijndael.

„Rijndael“ sudarytas sujungus jo kūrėjų – dviejų belgų kriptografų V. Rijmen ir J. Daemen – pavardžių skiemenis.

Veiksmai su baitais

AES kriptosistema atlieka veiksmus su baitais. Kiekvieną baitą, t. y. aštuonių bitų žodį $b = b_7b_6b_5b_4b_3b_2b_1b_0$, interpretuokime kaip daugianarį

$$b(x) = b_7x^7 + b_6x^6 + \dots + b_1x + b_0.$$

Du tokius daugianarius sudėję, vėl gausime tos pačios erdvės daugianarį. Imkime aštunto laipsnio daugianarį

$$f(x) = x^8 + x^4 + x^3 + x + 1$$

ir apibrėžkime daugianarių (baitų) sandaugą:

$$a(x) \times b(x) = a(x)b(x) \text{ dalybos iš } f(x) \text{ liekana.}$$

AES variantai

	Rakto ilgis	Bloko ilgis	Iteracijų skaičius
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

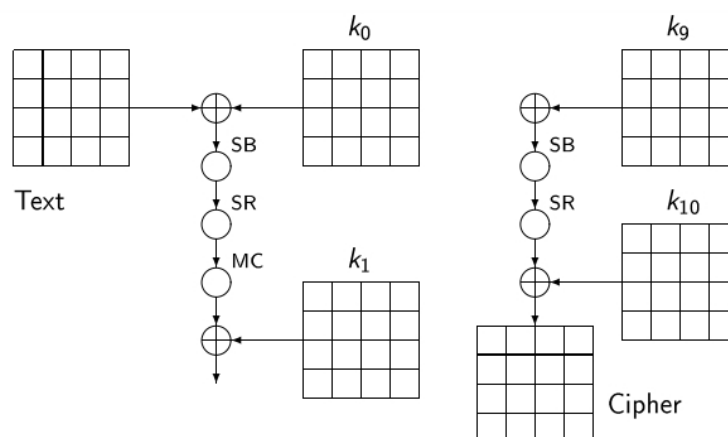
SQUARE schema

Pradinių duomenų blokas prieš pradedant transformacijas surašomas į lentelę.

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

AES duomenų blokas; lentelės elementai – aštuonių bitų ilgio žodžiai (baitai).

Bendra AES schema



AES-128 sudaro 10 vienodos struktūros žingsnių. Kiekvienai operacijai iš kriptosistemos bendro rakto sudaromas dalinis raktas. Šifravimas prasideda sudėties su pradžios raktu veiksmu. Pirmieji devyni žingsniai vienodi – atliekamos baitų keitimo (SB), eilučių postūmio (SR) ir stulpelių maišymo (MC) operacijos.

Baitų keitimo operacija

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Baitų keitimo operacijos matricinė išraiška. Antroji matricos eilutė gauta iš pirmosios, atlikus jos elementų postūmį, analogiškai iš antrosios eilutės gaunama trečioji ir t. t.

Baitų postūmio operacija

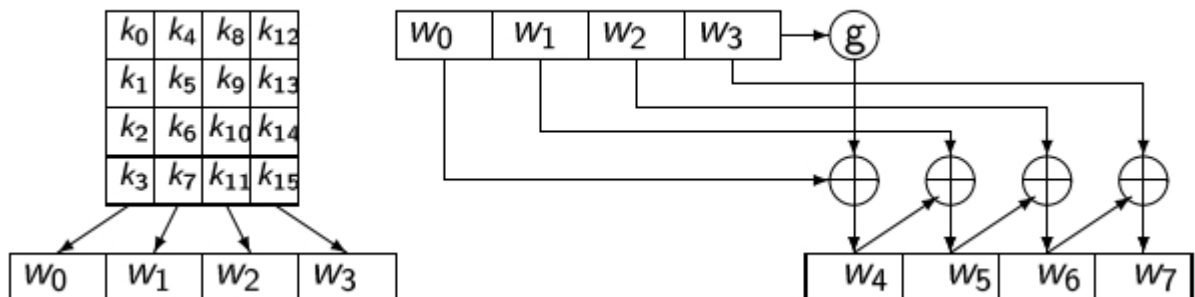
s ₀₀	s ₀₁	s ₀₂	s ₀₃	→	s ₀₀	s ₀₁	s ₀₂	s ₀₃
s ₁₀	s ₁₁	s ₁₂	s ₁₃		s ₁₁	s ₁₂	s ₁₃	s ₁₀
s ₂₀	s ₂₁	s ₂₂	s ₂₃		s ₂₂	s ₂₃	s ₂₀	s ₂₁
s ₃₀	s ₃₁	s ₃₂	s ₃₃		s ₃₃	s ₃₀	s ₃₁	s ₃₂

Stulpelių maišymo operacija

$$\begin{pmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix}.$$

AES stulpelių maišymo operacijos matricinė išraiška. Matricos elementus reikia interpretuoti kaip šešioliktaine sistema užrašytus baitus.

Raktų sudarymo operacija



Vienas rakto išplėtimo algoritmo ciklas. Pradinis AES raktas išsaugomas 32 bitų žodžiuose w_0, w_1, w_2, w_3 , o naudojantis jais sukuriama dar keturi žodžiai

Raktų sudarymo operacija

Rakto išplėtimo schemos funkcija g :

$$g(w) = SB(rot(w)) + R_j,$$

čia rot baitų postūmio operacija, $rot(b_0b_1b_2b_3) = b_1b_2b_3b_0$; SB – baitų keitimo operacija, apibrėžta anksčiau, o R_j – j -ojo žingsnio konstanta. Šios konstantos sudaromos pagal paprastą taisyklę (naudojama baitų daugyba):

$$R_j = r_j000000, \quad r_1 = 01, \quad r_j = 2 \cdot r_{j-1}.$$

2.7 Srautiniai šifrai

Srautiniai šifrai

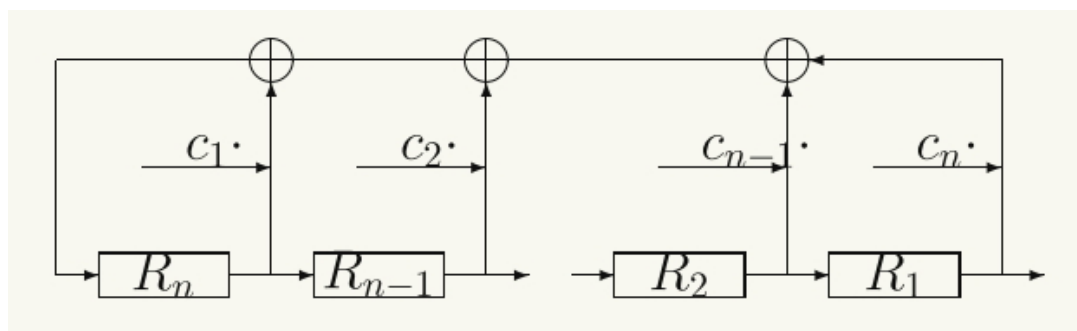
Tegu $M = m_1m_2\dots$ dvejetainės abėcėlės simbolių srautas, generuokime tokio pat ilgio rakto žodį $K = x_1x_2\dots$ ir apibrėžkime M šifrą taip:

$$C = e(M|K) = c_1c_2\dots, \quad c_i = m_i \oplus x_i, \quad i = 1, 2, \dots$$

Dešifravimas – ta pati XOR operacija, tik ją atlikti reikia su šifro ir rakto srautais:

$$M = d(C|K) = m_1m_2\dots, \quad m_i = c_i \oplus x_i, \quad i = 1, 2, \dots$$

Tiesiniai registrai



Tiesinių registrų sistema. Kiekviename žingsnyje atliekamas registrų bitų postūmis: pirmojo registro bitu papildomas generuojamas bitų srautas, antrojo registro bitas perrašomas į pirmąjį registrą, ..., n -ojo – į $n - 1$ -ąjį, o į n -ąjį registrą įrašoma registrų bitų tiesinė kombinacija.

Tiesinių registrų sistema

Jei

$$x(t) = \langle x_1(t), \dots, x_n(t) \rangle$$

yra sistemos padėtis laiko momentu t , tai sekančiame žingsnyje bus atlikti tokie veiksmai

$$x_i(t) = x_{i+1}(t), \quad 1 \leq i \leq n-1, \quad (1)$$

$$x_n(t+1) \equiv c_1 x_n(t) + \dots + c_n x_1(t) \pmod{2}, \quad (2)$$

čia $c_i \in \{0, 1\}$, $1 \leq i \leq n$. Sakysime, kad $c_n \neq 0$, nes priešingu atveju registrų sistemą galėtume sutrumpinti.

Tiesinių registrų sistema

Kiekviena žingsnyje žodis $x(t)$ (dvejetainis vektorius) yra atvaizduojamas į žodį $x(t+1)$:

$$x(t+1) = x(t)C, \quad C = \begin{pmatrix} 0 & 0 & \dots & 0 & c_n \\ 1 & 0 & \dots & 0 & c_{n-1} \\ 0 & 1 & \dots & 0 & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & c_1 \end{pmatrix}.$$

Periodinės sekos

Apibrėžimas. Elementų seką $\{y_i\}$ ($i = 0, 1, \dots$) vadinsime periodine, jeigu egzistuoja toks natūralusis skaičius p , kad su visais $i \geq 0$ teisinga lygybė $y_{i+p} = y_i$. Mažiausią natūralųjį skaičių p , su kuriuo visos lygybės teisingos vadinsime sekos periodu.

Teorema. Tiesinė n registrų sistema generuoja periodines sekas, kurių periodas yra ne didesnis už $2^n - 1$.

Primityvūs daugianariai

Apibrėžimas. n -ojo laipsnio daugianaris $f(x) \in \mathbb{F}_2[x]$ vadinamas primitiviuoju, jeigu jis yra neskaidus ir nėra jokio daugianario $x^d + 1$ su $d < 2^n - 1$ daliklis.

Rasti n -ojo laipsnio primitiviuosius daugianarius nėra paprastas algebros uždavinys. Tačiau žinoma, kad visiems natūraliesiems n jie egzistuoja.

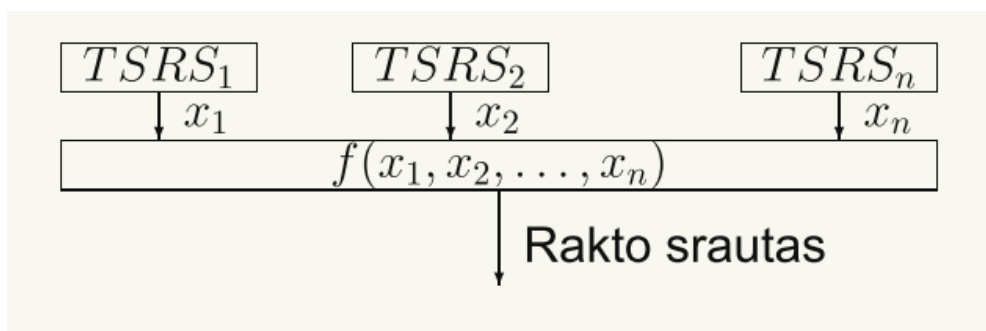
Maksimalaus periodo sekos

Apibrėžimas. Tiesinės registrų sistemos charakteringuoju daugianariu vadinsime daugianarį

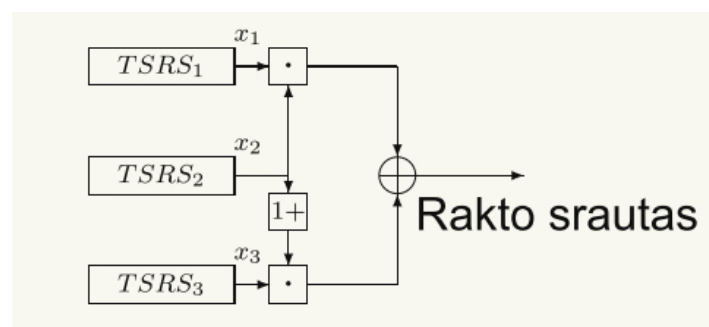
$$P_n(x) = 1 + c_1x + \dots + c_nx^n, c_n \neq 0.$$

Teorema. Tiesinė registrų sistema generuoja maksimalaus periodo seką tada ir tik tada, kai jos charakteringasis daugianaris yra primitivus.

Tiesinių registrų sistemų jungimas

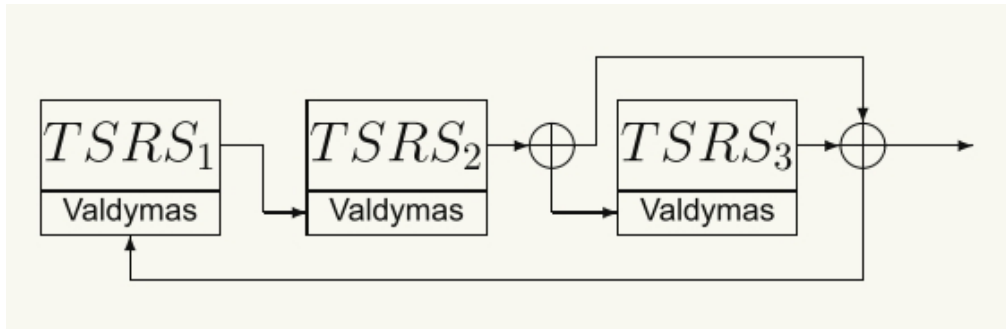


Kelių tiesinių registrų sistemų lygiagretus jungimas



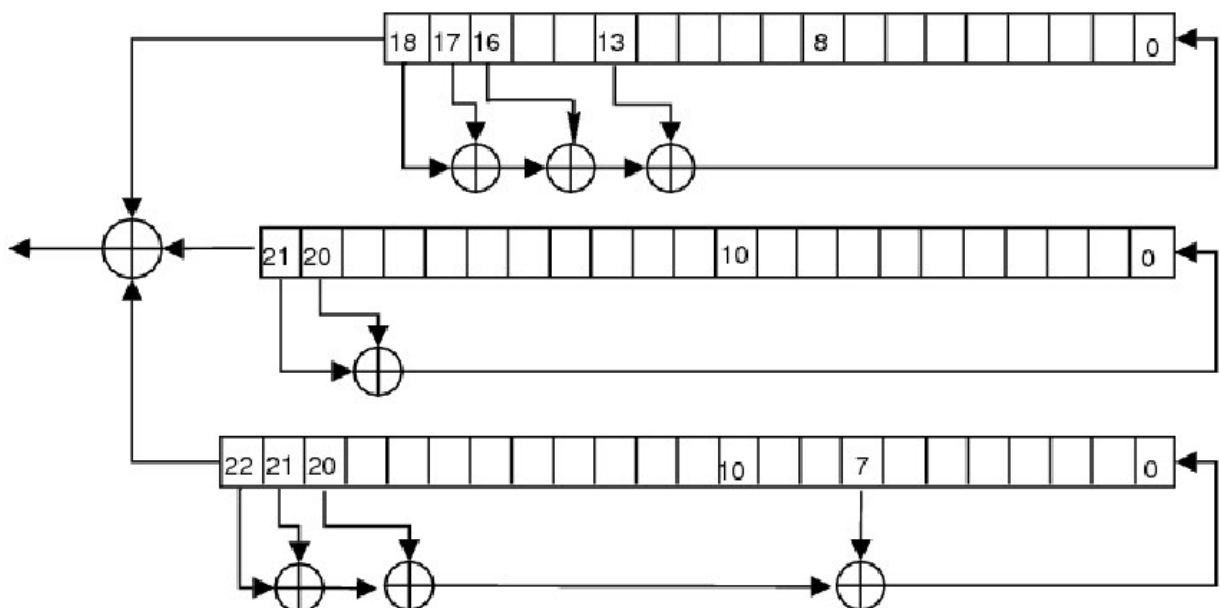
Geffe generatorius

Tiesinių registrų sistemų jungimas



Golmano tiesinių registrų sistemų grandinė. Jeigu į tiesinės registrų sistemos „valdymo“ skyrių perduoto bito reikšmė lygi vienetui, sistema generuoja eilinį bitą ir atlieka registrų turinių postūmį; jeigu valdymo bitas lygus nuliui, registrų turiniai nepasikeičia. Rakto srautas – dviejų paskutinių registrų bitų suma.

A5/1



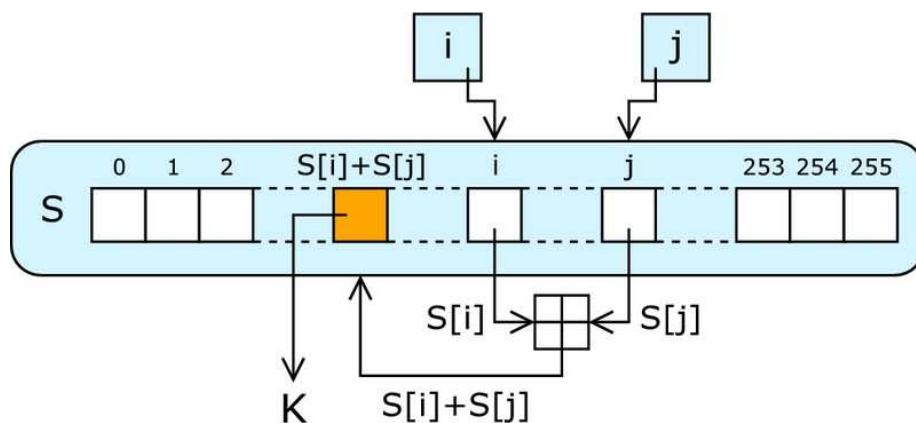
A5/1 kriptosistema

RC4

Raktas: l baitų seka $K[0], \dots, K[l-1]$. Inicializacija:

1. $j:=0$
2. for $i=0$ to 255 do
3. $S[i]:=i$ end
4. for $i=0$ to 255 do
5. $j:=j+S[i+K[i \bmod l]]$
6. $S[i] \leftrightarrow S[j]$ end $i:=0$ $j:=0$

RC4 šifravimas



1. $i:=i+1$ $j:=j+S[i]$
 2. $S[i] \leftrightarrow S[j]$
- $S[S[i] + S[j]] \mapsto$ rakto srautas

Statistiniai testai

Tegu X_1, X_2, \dots nepriklausomi atsitiktiniai dydžiai, su vienodomis tikimybėmis įgyjantys reikšmes iš aibės $\{0, 1\}$, t. y. generuojantys tikrai atsitiktinius bitų srautus.

Uždavinys

Gauta bitų seką $\mathbf{x} = x_1 x_2 \dots x_n$.

Reikia priimti vieną iš dviejų hipotezių:

H_0 : \mathbf{x} yra tipinė dydžių X_1, X_2, \dots, X_n generuota seka,

H_1 : \mathbf{x} nėra tipinė dydžių X_1, X_2, \dots, X_n generuota seka.

Statistiniai testai

Testo ideologija:

sudaromas atsitiktinis dydis $T = T(X_1, X_2, \dots, X_n)$, kurio pasiskirstymas yra toks pat (dažniausiai „praktiškai beveik toks pat“) kaip žinomo atsitiktinio dydžio X .

Pasirenkamas mažas skaičius α , randamas

$$z_\alpha, \alpha = P(|X| > z_\alpha).$$

Naudojant tiriamą seką $\mathbf{x} = x_1 x_2 \dots x_n$ apskaičiuojama

$$t = T(x_1, x_2, \dots, x_n).$$

Jei $t > z_\alpha$ hipotezė H_0 atmetama.

Tikimybė $p = P(|X| > t)$ vadinama p -reikšme. Kuo ji mažesnė, tuo „labiau pagrįstas“ hipotezės H_0 atmetimas.

Standartinis normalusis dydis

Atsitiktinis dydis X vadinamas standartiniu normaliuoju, jei

$$P(X < u) = \int_{-\infty}^u p_X(x) dx, \quad p_X(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}.$$

Žymime $X \sim \mathcal{N}(0, 1)$. Tada p -reikšmės skaičiuojamos taip:

$$p = P(|X| > t) = 2 \int_t^{+\infty} p_X(x) dx$$

Dydis, pasiskirstęs pagal $\chi^2(m)$ dėsnį

Atsitiktinis dydis X vadinamas dydžiu, pasiskirsčiusiu pagal $\chi^2(m)$ dėsnį, jei

$$P(X < u) = \int_{-\infty}^u p_X(x) dx, \quad p_X(x) = \frac{x^{n-1} e^{-\frac{x^2}{2}}}{2^{n/2-1} \Gamma(n/2)}, \quad x > 0..$$

Žymime $X \sim \chi^2(m)$. Tada p -reikšmės skaičiuojamos taip:

$$p = P(|X| > t) = \int_t^{+\infty} p_X(x) dx$$

Pavienių bitų testas

Tiriame bitų seką $\mathbf{x} = x_1 x_2 \dots x_n$.

Tegu N_0 yra nulių skaičius atsitiktinių bitų sekoje, o N_1 – vienetų. Tada dydžio

$$T_1 = \frac{(N_1 - N_0)^2}{n}$$

pasiskirstymo dėsnis, kai $n \geq 10$ yra labai artimas dėsniai $\chi^2(1)$.

Bitų porų testas

Tiriame bitų seką $\mathbf{x} = x_1 x_2 \dots x_n$. Tegu dydžių N_0, N_1 reikšmės yra tos pačios kaip pavienių bitų teste, o $N_{00}, N_{01}, N_{10}, N_{11}$ yra atitinkamai bitų blokų 00, 01, 10, 11 kiekiai bitų sekoje.

Kadangi poros gali turėti vieną bendrą bitą, tai

$$N_{00} + N_{01} + N_{10} + N_{11} = n - 1.$$

Apibrėžkime statistiką

$$T_2 = \frac{4}{n-1} \left(N_{00}^2 + N_{01}^2 + N_{10}^2 + N_{11}^2 \right) - \frac{2}{n} \left(N_0^2 + N_1^2 \right) + 1.$$

Kai $n \geq 21$ statistikos T_2 pasiskirstymo dėsnis artimas dėsniai $\chi^2(2)$.

Pokerio testas

Tiriame bitų seką $\mathbf{x} = x_1 x_2 \dots x_n$. Fiksuokime m ($m < n$); visų skirtingų žodžių aibė yra $\{a_1, a_2, \dots, a_{2^m}\}$. Padalykime bitų seką į $k = \lfloor \frac{n}{m} \rfloor$ m ilgio žodžių ir, peržiūrėję juos, nustatykite, kiek kartų pasitaiko žodžiai a_1, a_2, \dots, a_{2^m} . Šių žodžių pasitaikymo kiekius pažymėkime N_1, N_2, \dots, N_{2^m} . Dabar jau galime sudaryti statistiką

$$T_3 = \frac{2^m}{k} \sum_{i=1}^{2^m} N_i^2 - k.$$

Jeigu $k \geq 5 \cdot 2^m$, tai T_3 pasiskirstymo dėsnis artimas $\chi^2(2^m - 1)$.

Blokų testas

Tiriame bitų seką $\mathbf{x} = x_1 x_2 \dots x_n$. Pažymėkime F_r blokų $10_r 1$ skaičių bitų sekoje, o G_r blokų $01_r 0$ skaičių. Pažymėkime

$$E_i = \frac{n - i + 3}{2^{i+2}}$$

ir k – didžiausią natūrinį skaičių, su kuriuo $E_k \geq 5$. Statistiką apibrėšime taip:

$$T_4 = \sum_{i=1}^k \left\{ \frac{(F_i - E_i)^2}{E_i} + \frac{(G_i - E_i)^2}{E_i} \right\}.$$

Statistikos T_4 pasiskirstymo dėsnis yra artimas $\chi^2(2k - 2)$.

Autokoreliacijos testas

Tiriame bitų seką $\mathbf{x} = x_1x_2 \dots x_n$. Tegu $1 \leq d \leq \lfloor n/2 \rfloor$ ir

$$X(d) = \sum_{i=1}^{n-d+1} X_i \oplus X_{i+d-1}.$$

Dydis X_d yra lygus nesutampančių bitų skaičiui, kai lyginame bitų seką su ja pačia, paslinkta per $d - 1$ poziciją į kairę (x_1 lyginamas su x_d). Jeigu $n - d \geq 10$, tai statistikos

$$T_5 = \frac{2X(d) - n + d}{\sqrt{n - d}}$$

pasiskirstymo dėsnis yra artimas standartiniam normaliajam dėsniai $\mathcal{N}(0, 1)$.

NIST statistinių testų paketas

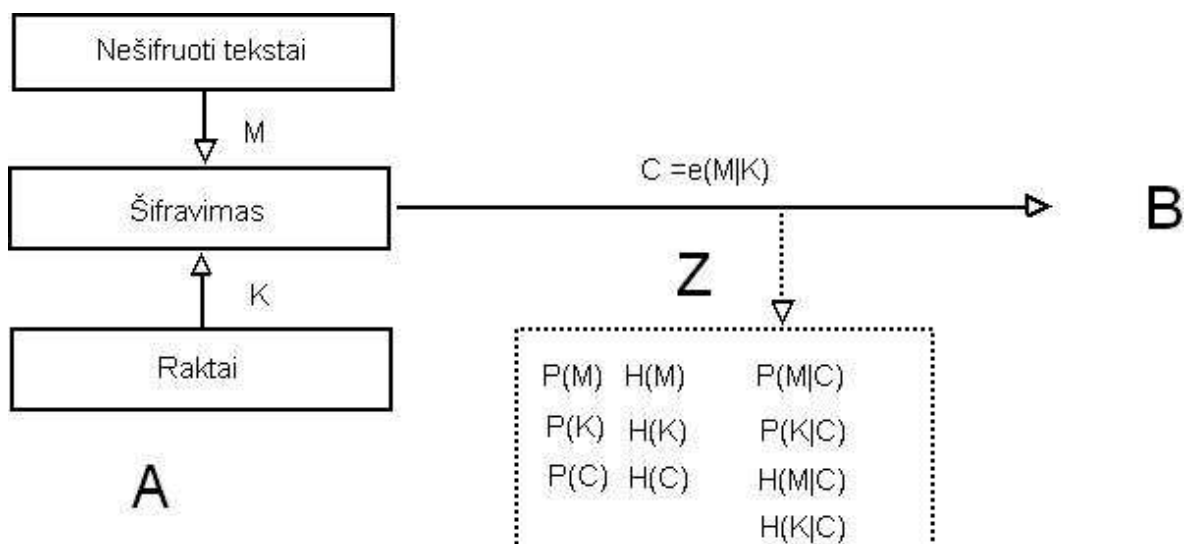
Standartinių testų rinkinys



Norint naudotis – reikia sukompiliuoti C kalbos kodą!

2.8 Kriptosistemų saugumas informacijos teorijos požiūriu

E. Shannono požiūris



Besąlygiškai saugi kriptosistema

Apibrėžimas. Kriptosistema vadinama besąlygiškai saugia, jei su visomis galimomis M ir K reikšmėmis

$$P(\mathcal{M} = M) = P(\mathcal{M} = M | \mathcal{C} = C).$$

Būtina besąlygiško saugumo sąlyga

Teorema. Jei kriptosistema yra besąlygiškai saugi, tai raktų aibė yra ne mažesnės galios kaip pranešimų aibė.

Entropija

X, Y atsitiktiniai dydžiai

$$H(X) = \sum_x P(X = x) \log_2 \frac{1}{P(X = x)}$$

$$\begin{aligned} H(X|Y = y) &= \sum_x P(X = x|Y = y) \log_2 \frac{1}{P(X = x|Y = y)}, \\ H(X|Y) &= \sum_x H(X|Y = y) P(Y = y) \end{aligned}$$

Entropijos savybės

Teorema.

- $H(X|Y) \leq H(X)$
- $H(X|Y) = H(X)$ tada ir tik tada, kai X, Y yra nepriklausomi;
- $H(X, Y) = H(Y) + H(X|Y)$;
- jei $X = f(Y)$, tai $H(X|Y) = 0$.

Išvada. Jei X_1, X_2, \dots, X_n yra nepriklausomi atsitiktiniai dydžiai, tai

$$H(X_1, \dots, X_n) = H(X_1) + H(X_2) + \dots + H(X_n).$$

Besąlygiškai saugios kriptosistemos

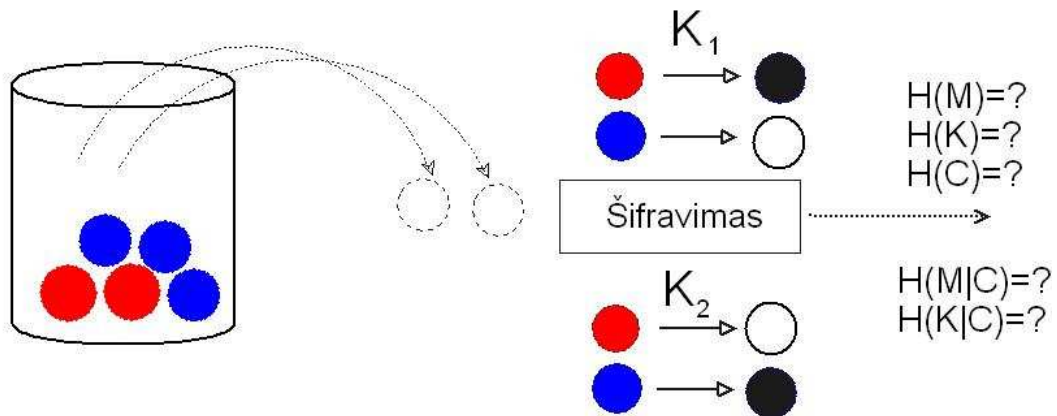
Teorema. Kriptosistema yra besąlygiškai saugi tada ir tik tada, kai $H(\mathcal{M}) = H(\mathcal{M}|\mathcal{C})$

Raktas „slaptesnis“ nei pranešimas

Teorema. Bet kokios kriptosistemos atveju

$$H(\mathcal{K}|\mathcal{C}) \geq H(\mathcal{M}|\mathcal{C}).$$

Pavyzdys



Rakto įminimo taškas

Pranešimų ir šifrų abėcėlė \mathcal{A} , raktų aibė \mathcal{K} .
Šifruojami atskiri simboliai, \mathcal{M}_n – n ilgio
pranešimas iš \mathcal{A} raidžių,

$$\mathcal{C}_n = e(\mathcal{M}_n | \mathcal{K}).$$

Teorema.

$$H(\mathcal{K} | \mathcal{C}_n) = H(\mathcal{M}_n) + H(\mathcal{K}) - H(\mathcal{C}_n)$$

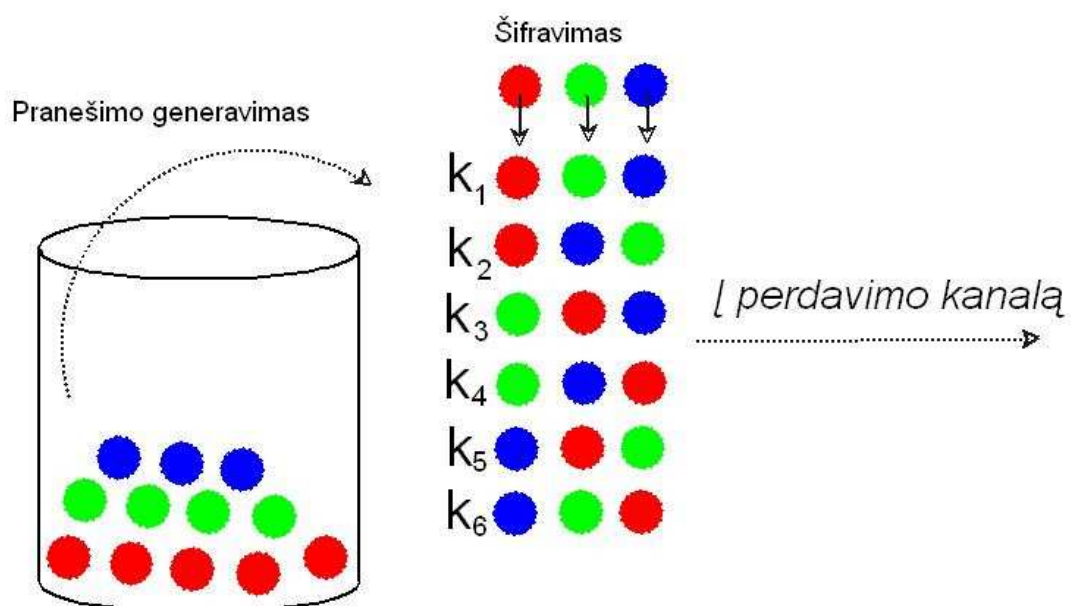
Rakto įminimo taškas

$$H(\mathcal{M}_N) + H(\mathcal{K}) - H(\mathcal{C}_N) = 0,$$

$$H(\mathcal{M}_N) = N \cdot H, \quad H(\mathcal{K}) = \log_2 |\mathcal{K}|,$$

$$H(\mathcal{C}_N) + N \cdot L \leq N \cdot \log_2 |\mathcal{A}|$$

Pavyzdys



2.9 Sudėtingumo teorijos pradmenys

Uždaviniai ir jų sprendimai

Uždavinys (problema): duomenys D ir užduotis arba klausimas, į kurį reikia pateikti atsakymą.

Duomenis ir atsakymą galime užrašyti dvejetainės abėcėlės $\mathcal{B} = \{0, 1\}$ simboliais. Visų dvejetainės abėcėlės žodžių aibę žymėsime \mathcal{B}^* .

Uždavinio sąvoka

Apibrėžimas. Uždaviniu vadinsime aibę $\pi \subset \mathcal{B}^* \times \mathcal{B}^*$, jei kiekvienam $X \in \mathcal{B}^*$ atsiras $Y \in \mathcal{B}^*$, kad $\langle X, Y \rangle \in \pi$. Jei $\langle D, A \rangle \in \pi$, tai D vadinsime įeities duomenimis, o A – atsakymu.

Uždavinio sąvoka

Apibrėžimas. Uždavinį $\pi \subset \mathcal{B}^* \times \mathcal{B}^*$, vadinsime funkcija, jei kiekvienam $X \in \mathcal{B}^*$ atsiras vienintelis $Y \in \mathcal{B}^*$, kad $\langle X, Y \rangle \in \pi$. Jei galimos tik dvi atsakymo A reikšmės, funkciją vadinsime išsprendžiamumo uždaviniu (problema).

Apibrėžimas. Išsprendžiamumo uždavinio $\pi \subset \mathcal{B}^* \times \mathcal{B}^*$ kalba vadinsime poaibį

$$\mathcal{L}_\pi = \{D : D \in \mathcal{B}^*, \langle D, T \rangle \in \pi\}.$$

Išsprendžiamumo uždavinį galime interpretuoti kaip klausimą, ar žodis $x \in \mathcal{B}^*$ įeina į kalbą \mathcal{L}_π .

Uždavinio sprendimas – Turingo mašina

Jei įvesties duomenys yra x , tai $t_M(x)$ reiškia mašinos operacijų, reikalingų atsakymui gauti, skaičių.

Apibrėžimas. Turingo mašinos M darbo laiku vadinsime funkciją $T_M : \mathbb{N} \rightarrow \mathbb{N}$, kurios reikšmė kiekvienam natūraliajam n yra lygi

$$T_M(n) = \max\{t_M(x) : |x| = n\}.$$

Pavyzdys - Euklido dalybos su liekana algoritmas

Pakanka skaičiuoti matematinės operacijas.

$$\begin{array}{ll} u = q_1v + r_1, & 0 < r_1 < v; \\ v = q_2r_1 + r_2, & 0 < r_2 < r_1; \\ r_1 = q_3r_2 + r_3, & 0 < r_3 < r_2; \\ \vdots & \vdots \\ r_{k-3} = q_{k-1}r_{k-2} + r_{k-1}, & 0 < r_{k-1} < r_{k-2}; \\ r_{k-2} = q_k r_{k-1}. \end{array}$$

Po k operacijų $(u, v) = r_{k-1}$.

1845 m. Lame įrodė: jei $0 < v < u < N$, tai

$$k \leq [\log_{\varphi}(\sqrt{5}N)] - 2,$$

čia $\varphi = (1 + \sqrt{5})/2$.

Polinominiai uždaviniai

Apibrėžimas. Algoritmas, kurio Tiuringo mašinos darbo laikas yra $T_M(n)$, vadinamas polinominio laiko algoritmu, jei egzistuoja daugianaris p , kiekvienam $n \in \mathbb{N}$ tenkinantis nelygybę $T_M(n) \leq p(n)$.

Sakysime, kad uždavinys priklauso polinominio laiko uždavinių klasei P, jei jos sprendimui žinomas polinominio laiko algoritmas.

Nepolinominiai uždaviniai

I uždavinys:

D: natūrinis skaičius n ;

U: ar n yra sudėtinis?

II uždavinys:

D: Grafas G ;

U: ar G yra Hamiltono grafas?

NP uždaviniai

Neformalus paaiškinimas

Tarkime, \mathbb{U} yra išsprendžiamumo uždavinys, kuriam spręsti polinominis algoritmas nežinomas. Tačiau, kai atsakymas, atitinkantis įvesties duomenis yra T (TAIP), tai šį atsakymą galima surasti per polinominį laiką, jeigu žinai papildomą informaciją (raktą).

Toks uždavinys vadinamas **NP-uždaviniu**.

NP uždaviniai

Formalus apibrėžimas

Apibrėžimas. Tarkime, kad $\pi \subset \mathcal{B}^*$ yra išsprendžiamumo uždavinio kalba. Sakysime, kad šis uždavinys yra NP uždavinys, jei egzistuoja funkcija $f : \mathcal{B}^* \times \mathcal{B}^* \rightarrow \{0, 1\}$, tokia, kad

- $x \in \pi$ tada ir tik tada, kai egzistuoja toks $y \in \mathcal{B}^*$, kad $f(x, y) = 1$;
- $f(x, y)$ skaičiuojama $|x|$ atžvilgiu polinominio laiko algoritmu.

Šiame apibrėžime žodis $y \in \mathcal{B}^*$ ir yra uždavinio sprendimo raktas, kurį reikia kaip nors įspėti.

Uždavinių keitimas

Neformalus paaiškinimas

Tarkime P_1, P_2 yra du išsprendžiamumo uždaviniai. Jeigu P_1 duomenis x polinominiu algoritmu galima pakeisti uždavinio P_2 duomenimis y ir atsakymas į y duomenis yra toks pat, kaip atsakymas į x duomenis, tai sakoma, kad uždavinys P_1 yra polinomiškai suvedamas į uždavinį P_2 .

Uždavinių keitimas

Formalus apibrėžimas

Apibrėžimas. Tarkime π_1, π_2 yra dviejų išsprendžiamumo uždavinių kalbos. Sakysime, kad pirmasis uždavinys yra polinomiškai suvedamas į antrąjį, jei egzistuoja polinominio laiko funkcija $\varphi : \mathcal{B}^* \rightarrow \mathcal{B}^*$, tenkinanti sąlygą: $x \in \pi_1$ tada ir tik tada, kai $\varphi(x) \in \pi_2$.

Cooko teorema

Teorema. Jei uždavinys P_1 yra polinomiškai suvedamas į P_2 , ir P_2 priklauso polinominių uždavinių klasei, tai ir P_1 priklauso šiai klasei.

Teorema. (Cooko) Egzistuoja NP uždavinys, į kurį polinomiškai galima suvesti bet kurį kitą NP uždavinį.

Milijono vertės uždavinys



NP pilnų uždavinių pavyzdžiai

Vienspalvis trikampis (monochromatic triangle)

- D: Grafas $G = \langle V, E \rangle$,
- U: Ar galima nuspalvinti visas grafo briaunas dviem spalvomis, kad iš tos pačios spalvos briaunų ir atitinkamų viršūnių negalėtume sudaryti vieno trikampio?

NP pilnų uždavinių pavyzdžiai

Kvadratiniai lyginiai

- D: natūralieji skaičiai a, b, c ;
- U: ar egzistuoja natūralusis skaičius x , $|x| < c$, kad $x^2 \equiv a \pmod{b}$?

NP pilnų uždavinių pavyzdžiai

Keliaujantis prekeivis

- D: miestų aibė C , atstumai tarp miestų $d(c_i, c_j)$, skaičius $B > 0$;
- U: ar egzistuoja būdas apeiti visus miestus, kad viso kelio ilgis neviršytų B ?

NP pilnų uždavinių pavyzdžiai

Dalumo palyginimas

- D: Du natūraliųjų skaičių rinkiniai $\{a_1, \dots, a_n\}$ ir $\{b_1, \dots, b_m\}$;
- U: ar yra toks natūralusis skaičius c , kad skaičių iš pirmojo rinkinio, kuriuos dalo c , yra daugiau nei analogiškų skaičių iš antrojo rinkinio?

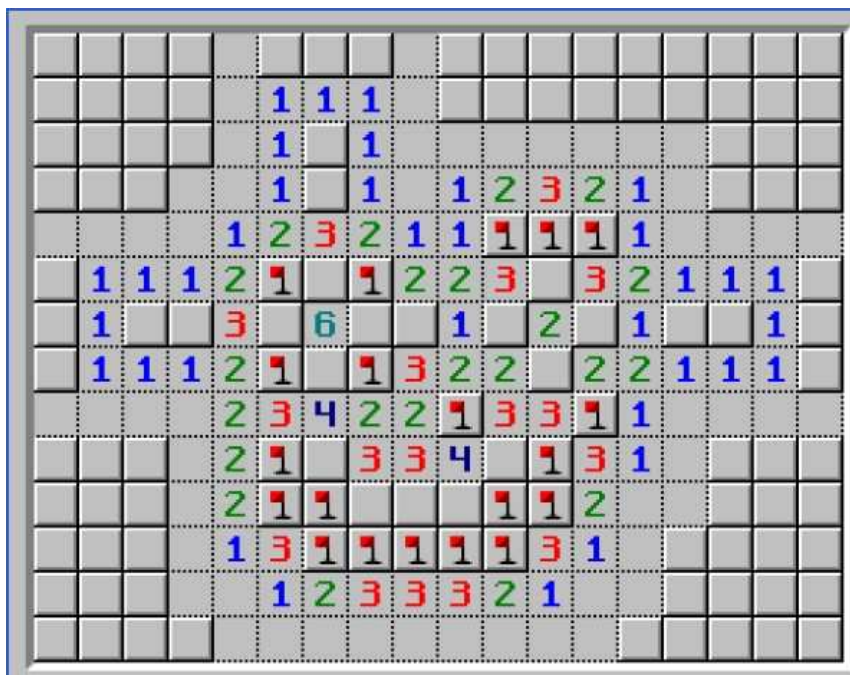
NP pilnų uždavinių pavyzdžiai

Diofanto lygtys

- D: natūralieji skaičiai a, b, c ;
- U: ar egzistuoja natūralieji skaičiai x, y , kad $ax^2 + by = c$?

NP pilnų uždavinių pavyzdžiai

Minesweeper



Ar duomenys atitinka kokį nors minų išdėstymą?

3. Viešojo rakto kriptografija

Euklido algoritmas

$$\begin{aligned}a &= q_0b + r_0, & 0 < r_0 < b, \\b &= q_1r_0 + r_1, & 0 < r_1 < r_0, \\r_0 &= q_2r_1 + r_2, & 0 < r_2 < r_1, \\&\dots\dots\dots \\r_{n-2} &= q_nr_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\r_{n-1} &= q_{n+1}r_n, \\r_n &= (a, b).\end{aligned}$$

Bendrojo daliklio išraiška

$$(a, b) = r_{n-2} + (-q_n)r_{n-1},$$

.....

$$(a, b) = ur_{k-2} + vr_{k-1},$$

$$(a, b) = vr_{k-3} + (u - vq_{k-1})r_{k-2},$$

.....

$$(a, b) = xa + yb.$$

Bendrojo daliklio išraiška

r_{i-1}, r_i	q_i	u_{i-1}, u_i
a, b		x, y
b, r_0	q_0	
r_0, r_1	q_1	
...	...	
r_{k-2}, r_{k-1}	q_{k-1}	$v; u - vq_k.$
r_{k-1}, r_k	q_k	$u; v$
...	...	
r_{n-2}, r_{n-1}	q_{n-1}	$1; -q_n$
r_{n-1}, r_n	q_n	

Pavyzdys

57; 10		3; -17
10; 7	5	-2; 3
7; 3	1	1; -2
3; 1	2	
0		

$$(57, 10) = 3 \cdot 57 + (-17) \cdot 10$$

Eulerio funkcija

Apibrėžimas

Apibrėžimas. Funkcija

$$\varphi(n) = |\{m : 1 \leq m < n, (m, n) = 1\}|$$

vadinama Eulerio funkcija.

Euleris – tariama Oileris.

Eulerio funkcijos savybės

Teorema. Jei $(m, n) = 1$, tai

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Teorema.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Svarbios teoremos

Teorema. (Fermat) Jei $(a, n) = 1$, tai $a^{\varphi(n)} - 1 = tn$, t. y. $a^{\varphi(n)} - 1$ dalijasi iš n .

Teorema. (Eulerio) Jei p yra pirminis skaičius, $(a, p) = 1$, tai $a^{p-1} - 1$ dalijasi iš p

Skaičiavimai moduliu n

Žiedai, grupės, kūnai

$$\begin{aligned}\mathbb{Z}_n &= \{0, 1, 2, \dots, n-1\}, \\ \mathbb{Z}_n^* &= \{a : a \in \mathbb{Z}_n, (a, n) = 1\}, \\ \mathbb{Z}_p^* &= \{1, 2, \dots, p-1\}, \quad \text{jei } p \text{ pirminis}\end{aligned}$$

Sudėties ir daugybos veiksmai \mathbb{Z}_n

Jei $a - b$ dalijasi iš n , rašome

$$a \equiv b \pmod{n}$$

Tokį sąryšį vadiname lyginiu.

Veiksmų su lyginiais savybės!

Svarbios teoremos

Teorema. (Fermat) Jei $(a, n) = 1$, tai $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Teorema. (Eulerio) Jei p yra pirminis skaičius, $(a, p) = 1$, tai $a^{p-1} \equiv 1 \pmod{p}$.

Žiedai, grupės, kūnai

\mathbb{Z}_n su sudėties ir daugybos veiksmais moduliu n yra žiedas.

Atvirkštinius elementus turi tik \mathbb{Z}_n^* elementai.

Atvirkštinius elementus galima rasti Euklido algoritmu. Aibė \mathbb{Z}_n^* su daugybos veiksmu sudaro grupę.

Jei p – pirminis skaičius, tai \mathbb{Z}_p yra kūnas.

Kinų liekanų teorema

Duoti skaičiai $y_1, y_2, \dots, y_k, n_1, n_2, \dots, n_k$.
Ieškome tokio skaičiaus y , kad būtų

$$y \equiv y_1 \pmod{n_1}, \dots, y \equiv y_k \pmod{n_k}.$$

Teorema. Tegu n_1, n_2, \dots, n_k yra tarpusavyje pirminiai skaičiai, y_1, y_2, \dots, y_k bet kokie skaičiai, $n = n_1 n_2 \dots n_k, m_i = n/n_i$, o $d_i m_i \equiv 1 \pmod{n_i}$. Tada skaičius

$$y = y_1 d_1 m_1 + y_2 d_2 m_2 + \dots + y_k d_k m_k$$

tenkina visus lyginius $y \equiv y_i \pmod{n_i}$.

Greitasis kėlimo laipsniu algoritmas

$$\begin{aligned}31 &= 1 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4, \\10^{31} &= 10^1 \cdot 10^2 \cdot (10^2)^2 \cdot ((10^2)^2)^2 \cdot (((10^2)^2)^2)^2,\end{aligned}$$

$$\begin{aligned}10^2 &\equiv 7 \pmod{31}, & 7^2 &\equiv 18 \pmod{31}, \\18^2 &\equiv 14 \pmod{31}, & 14^2 &\equiv 10 \pmod{31}, \\10^{31} &\equiv 10 \cdot 7 \cdot 18 \cdot 14 \cdot 10 \equiv 25 \pmod{31}.\end{aligned}$$

Ciklinė grupė \mathbb{Z}_p^*

Tegu p yra pirminis skaičius. Tada bet kokiam $a, (a, p) = 1$ teisingas lyginys $a^{p-1} \equiv 1 \pmod{p}$, t. y. $a^{p-1} = 1$ daugybos modulių p atžvilgiu.

Egzistuoja toks $g \in \mathbb{Z}_p$, kad

$$\{g^0, g^1, \dots, g^{p-1}\} = \mathbb{Z}_p^*.$$

Tokį g vadinsime generuojančiu elementu arba primityviaja vieneto šaknimi modulių p .

Primityvioji vieneto šaknis

Teorema. Skaičius g yra primitivioji vieneto šaknis moduliu p tada ir tik tada, kai kiekvienam netrivialiajam $p - 1$ dalikliui d
 $g^d \not\equiv 1 \pmod{p}$.

Kvadratiniai lyginiai

Apibrėžimas. Skaičius a vadinamas kvadratinio lyginio moduliu n , jei lyginys $x^2 \equiv a \pmod{n}$ turi sprendinį.

Kai n yra pirminis skaičius, tirti lyginio $x^2 \equiv a \pmod{n}$ sprendinių egzistavimą patogiau naudojantis Ležandro (Legendre) ir Jakobio simboliais.

Ležandro simbolis

Apibrėžimas. Tegu q yra pirminis skaičius, Ležandro simboliu vadinama funkcija

$$\left(\frac{a}{q}\right) = \begin{cases} 0, & \text{jei } a \equiv 0 \pmod{q}, \\ 1, & \text{jei } x^2 \equiv a \pmod{q} \text{ turi sprendinį,} \\ -1, & \text{jei } x^2 \equiv a \pmod{q} \text{ neturi sprendinio.} \end{cases}$$

Ležandro simbolio savybės

Teorema.

$$\begin{aligned} \left(\frac{a^2}{q}\right) &= 1, & \left(\frac{ab}{q}\right) &= \left(\frac{a}{q}\right) \left(\frac{b}{q}\right), \\ \left(\frac{a}{q}\right) &\equiv a^{(q-1)/2} \pmod{q}, & \left(\frac{a+kq}{q}\right) &= \left(\frac{a}{q}\right), \\ \left(\frac{-1}{q}\right) &= (-1)^{(q-1)/2}, & \left(\frac{2}{q}\right) &= (-1)^{(q^2-1)/8}. \end{aligned}$$

Gauso dėsnis

Teorema. Su bet kokiais skirtingais pirminiais skaičiais p, q teisinga lygybė

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Svarbus atvejis

Teorema. Jei p - pirminis skaičius, $p \equiv 3 \pmod{4}$ ir lyginys $x^2 \equiv a \pmod{p}$ turi sprendinį, tai vienas iš sprendinių yra

$$x_0 \equiv a^{\frac{p+1}{4}} \pmod{p}.$$

Kuprinės kriptosistema

Kuprinės uždavinys

ID: natūraliųjų skaičių (svorių) rinkinys

$W = \{w_1, w_2, \dots, w_n\}$, natūralusis skaičius w .

U: ar egzistuoja skaičiai $x_i \in \{0, 1\}$, kad

$$w = x_1 w_1 + x_2 w_2 + \dots + x_n w_n?$$

Ar iš turimų svorių galima sudėti norimo svorio kuprinę?

Sparčiai didėjantys svoriai

Apibrėžimas. Sakysime, kad skaičiai w_1, w_2, \dots, w_n sudaro sparčiai didėjančią seką, jei visiems $i > 1$ teisinga nelygybė

$$w_1 + w_2 + \dots + w_{i-1} < w_i.$$

Teorema. Jei kuprinės $W = \{w_1, w_2, \dots, w_n\}$ svoriai sudaro sparčiai didėjančią seką, tai kuprinės uždavinys sprendžiamas polinominiu algoritmu.

Spartus kuprinės iškraustymas

Tegu v – natūralusis skaičius. Ieškosime jo išraiškos

$$v = x_1 w_1 + x_2 w_2 + \dots + x_n w_n, \quad x_i \in \{0, 1\}.$$

Uždavinio sprendimo algoritmą galima užrašyti taip:

- $w := v, j := n$;
- jei $w \geq w_j$, tai $x_j = 1$; jei $w < w_j$, tai $x_j = 0$; $w := w - x_j w_j$;
- jei $w = 0$, tai išraiška rasta; jei $w \neq 0, j = 0$, išraiška neegzistuoja; kitais atvejais reikia kartoti 2 žingsnį.

Kuprinės ir šifrai

Turint svorių sistemą $W = \{w_1, w_2, \dots, w_n\}$ galima taip šifruoti nulių-vienetų blokus:

$$x_1x_2 \dots x_n \rightarrow c = x_1w_1 + x_2w_2 + \dots + x_nw_n.$$

Keblumai!

Vieną iš sprendimų 1976 metais pasiūlė Merkle ir Hellmanas.

Merkle-Hellmano kuprinės kriptosistema

Pranešimų aibė $\mathcal{M} = \{0, 1\}^n$, šifrų aibė $\mathcal{C} \subset \mathbb{N}$.

Privatusis raktas: $K_p = \langle W, s \rangle$, čia $W = \langle w_1, w_2, \dots, w_n \rangle$ – sparčiai didėjanti svorių sistema;

$$w_1 + w_2 + \dots + w_n < p, \quad (s, p) = 1.$$

Viešasis raktas: $K_v = \langle v_1, v_2, \dots, v_n \rangle$, $v_i \equiv w_i s^{-1} \pmod{p}$.

Šifravimas: $C = e(m_1 m_2 \dots m_n | K_v) = m_1 v_1 + \dots + m_n v_n$.

Dešifravimas: $C_1 \equiv Cs \pmod{p}$, $C_1 = m_1 w_1 + \dots + m_n w_n$,
 $m_1 \dots m_n = d(C | K_p)$.

RSA

RSA



Ronald Rivest, Adi Shamir, Leonard Adleman

RSA kriptosistema

Pranešimų ir šifrų aibės $\mathcal{M} = \mathcal{C} = \mathbb{Z}_n$, $n = pq$, skaičiai p, q yra pirminiai.

Privatusis raktas:

$$K_p = \langle d \rangle, (d, \varphi(n)) = 1, \varphi(n) = (p-1)(q-1).$$

Viešasis raktas: $K_v = \langle n, e \rangle$, $ed \equiv 1 \pmod{\varphi(n)}$.

Šifravimas: $C = e(M|K_v) \equiv M^e \pmod{n}$.

Dešifravimas: $M = d(C|K_p) \equiv C^d \pmod{n}$.

RSA hipotezė

RSA kriptanalizės problema ekvivalenti skaičių skaidymo pirminiais daugikliais problemai.

Skaidymo daugikliais uždavinys

The RSA-155 Challenge



■ The Effort

- 512 bit number (155 decimal digits)
- factored on August 22, 1999 after 7 months of cracking
- 300 workstations and Pentium PCs, 1 Cray supercomputer

```
109417386415705274218097073220403576120
037329454492059909138421314763499842889
347847179972578912673324976257528997818
33797076537244027146743531593354333897
=
102639592829741105772054196573991675900
716567808038066803341933521790711307779
*
106603488380168454820927220360012878679
207958575989291522270608237193062808643
```

RSA saugumas

Teorema. Jeigu $K_v = \langle n, e \rangle$, $K_p = \langle d \rangle$ yra RSA kriptosistemos raktai ir p, q, d tenkina sąlygas

$$q < p < 2q, \quad d < \frac{1}{3}n^{\frac{1}{4}},$$

tai iš viešojo rakto polinominiu algoritmu galima rasti privatųjį.

RSA saugumas

Teorema. Jeigu žinomi abu RSA kriptosistemos raktai $K_v = \langle n, e \rangle$ ir $K_p = \langle d \rangle$, tai n galima išskaidyti naudojant tikimybinį polinominį algoritmą.

RSA saugumas

Galime surasti tokią išraišką: $ed - 1 = 2^s t$, $(2, t) = 1$. Parinkime a , $(a, n) = 1$, ir skaičiuokime:

$$a_0 \equiv a^t \pmod{n}, \quad a_1 \equiv a_0^2 \pmod{n}, \quad \dots \quad a_i \equiv a_{i-1}^2 \pmod{n}, \dots$$

Kuris nors iš elementų a_j bus lygus 1. Tarkime, v yra mažiausias indeksas, su kuriuo

$$a_{v-1} \not\equiv 1 \pmod{n}, \quad a_v \equiv 1 \pmod{n}.$$

$$a_v \equiv a^{2^v t} \equiv a_{v-1}^2 \pmod{n}, \quad a_v - 1 \equiv (a_{v-1} - 1)(a_{v-1} + 1) \equiv 0 \pmod{n}.$$

Sandauga $(a_{v-1} - 1)(a_{v-1} + 1)$ dalijasi iš n ; jeigu nei vienas iš abiejų daugiklių nesidalytų iš n , tai vienas turėtų dalytis iš p , kitas iš q . Tada Euklido algoritmu surastume:

$$p = (a_{v-1} - 1, n), \quad q = (a_{v-1} + 1, n).$$

Rabino kriptosistema

Rabino kriptosistema

Privatusis raktas. $K_{pr} = \langle p, q \rangle$, p, q – pirminiai skaičiai,
 $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$.

Viešasis raktas. $K_v = \langle n \rangle, n = pq$.

Šifravimas ir dešifravimas

Šifravimas. Tekstai – skaičiai $m \in \mathbb{Z}_n$,

$$c = e(m|K_v) \equiv m^2 \pmod{n}.$$

Dešifravimas.

$$\begin{aligned} m_1 &\equiv c^{\frac{p+1}{4}} \pmod{p}, & m_2 &\equiv c^{\frac{q+1}{4}} \pmod{q}, \\ uq &\equiv 1 \pmod{p}, & vp &\equiv 1 \pmod{q}, \\ m &\equiv \pm m_1 uq \pm m_2 vp \pmod{n} \end{aligned}$$

Diskretusis logaritmas

Diskrečiojo logaritmo apibrėžimas

Apibrėžimas. Tegu p – pirminis skaičius, o g – generuojantis \mathbb{Z}_p^* elementas. Skaičiaus $a \in \mathbb{Z}_p^*$ diskrečiuoju logaritmu pagrindu g vadinamas skaičius x

$$g^x = a, \quad 0 \leq x \leq p-2.$$

Diskretusis logaritmas žymimas: $x = \log_g a$.

Shankso algoritmas

Tegu p – pirminis, $m = \lceil \sqrt{p-1} \rceil$, g – generuojantis elementas moduliui p .

Jei $y = \log_g x$, tai

$$y = mj + i, \quad 0 \leq j < m, 0 \leq i < m.$$

Shankso algoritmas

Išankstiniai skaičiavimai. Lentelė

$$L_1 : \quad \langle j, g^{mj}(\bmod p) \rangle, \quad 0 \leq j < m$$

Logaritmo skaičiavimas. Duotasis skaičius x .

$$L_2 : \quad \langle i, xg^{-i}(\bmod p) \rangle, \quad 0 \leq i < m.$$

Suraskime lentelėse L_1, L_2 poras su ta pačia antrąja komponente: $\langle j, y \rangle \in L_1, \langle i, y \rangle \in L_2$. Tada gausime:

$$g^{mj} = xg^{-i}, \quad x = g^{mj+i}, \quad \log_g x \equiv mj + i \pmod{p-1}.$$

ElGamalio kriptosistema

Raktų sudarymas. Tegu p – pirminis skaičius, g generuojantis elementas moduliu p , $0 < a \leq p-1$.

$$K_v = \langle p, g, \beta \rangle, \quad \beta \equiv g^a \pmod{p}, \quad K_p = \langle a \rangle.$$

Šifravimas. Pranešimų aibė $\mathcal{M} = \mathbb{Z}_p^*$. Parenkamas skaičius $k \in \mathbb{Z}_p^*$, pranešimo M šifras sudaromas taip:

$$C_1 \equiv g^k \pmod{p}, C_2 \equiv M\beta^k \pmod{p} \\ e(M, K_v) = \langle C_1, C_2 \rangle = C.$$

Dešifravimas. Šifras $C = \langle C_1, C_2 \rangle$ dešifruojamas taip:

$$d(C, K_p) \equiv C_2(C_1^a)^{-1} \pmod{p}.$$

Blumo-Goldwasserio kriptosistema

Raktai

Parenkami pirminiai skaičiai p, q , tokie, kad $p, q \equiv 3 \pmod{4}$, apskaičiuojama sandauga $n = pq$

$$K_v = \langle n \rangle, K_p = \langle p, q \rangle.$$

Pranešimų aibė

$$\mathcal{M} = \{m_1 m_2 \dots m_t : m_i \in \{0, 1\}^h\}, \quad t \geq 1, \quad h \leq \lceil \log_2 \log_2 n \rceil$$

Blumo-Goldwasserio kriptosistema

Šifravimas

Pranešimas $M = m_1 m_2 \dots m_t$, r - atsitiktinis skaičius.

$$x_0 \equiv r^2 \pmod{n}$$

bloko m_i šifravimas

$$x_i \equiv x_{i-1}^2 \pmod{n}$$

p_i yra h dešiniųjų x_i dvejetainės išraiškos bitų blokas

$$c_i = p_i \oplus m_i$$

Šifras $C = \langle c_1 c_2 \dots c_t, x_{t+1} \rangle$, $x_{t+1} \equiv x_t^2 \pmod{n}$.

Blumo-Goldwasserio kriptosistema

Dešifravimas

Šifro $C = \langle c_1 c_2 \dots c_t, x_{t+1} \rangle$ dešifravimas

$$d \equiv ((p+1)/4)^{t+1} \pmod{p-1},$$

$$e \equiv ((q+1)/4)^{t+1} \pmod{q-1},$$

$$u \equiv x_{t+1}^d \pmod{p}$$

$$v \equiv x_{t+1}^e \pmod{q}$$

$$x_0 \equiv u \pmod{p}, x_0 \equiv v \pmod{q}$$

$$x_i \equiv x_{i-1}^2 \pmod{n}$$

p_i yra h dešiniųjų x_i dvejetainės išraiškos bitų blokas

$$m_i = p_i \oplus c_i$$

Skaitmeniniai parašai

Skaitmeninių parašų schema

Skaitmeninių parašų schema:

tekstų aibė \mathcal{M} , skaitmeninių parašų aibė \mathcal{P} , raktų $K = \langle K_v, K_p \rangle$ aibė \mathcal{K} ir parašų sudarymo bei tikrinimo algoritmų šeimos

$$\begin{aligned} \text{sig}(\cdot|K_p) &: \mathcal{M} \rightarrow \mathcal{P}, \\ \text{ver}(\cdot|K_v) &: \mathcal{M} \times \mathcal{P} \rightarrow \{0,1\}. \end{aligned}$$

Jeigu $y \in \mathcal{P}$ pateikiamas kaip teksto $x \in \mathcal{M}$ parašas, tai parašas pripažįstamas galiojančiu, jeigu $\text{ver}(x,y|K_v) = 1$, ir pripažįstamas negaliojančiu, jei $\text{ver}(x,y|K_v) = 0$. Teisingai sudarytas parašas turi būti priimamas:

$$\text{ver}(x, \text{sig}(x|K_p)|K_v) = 1.$$

Kriptosistemos ir skaitmeniniai parašai

Beveik kiekvieną viešojo rakto kriptosistemą galima paversti skaitmeninių parašų schema: pasirašymas – šifravimas, parašo tikrinimas – dešifravimas.

RSA skaitmeninis parašas

Tekstų aibė \mathbb{Z}_n , $n = pq$, p, q – du pakankamai dideli pirminiai skaičiai.

Privatusis parašams sudaryti skirtas raktas: $K_p = \langle d \rangle$,
 $(d, \varphi(n)) = 1$.

Viešasis parašams tikrinti skirtas raktas: $K_v = \langle n, d \rangle$,
 $ed \equiv 1 \pmod{\varphi(n)}$.

Parašo sudarymas: tekstas $x \in \mathbb{Z}_n$, jo parašas $y \equiv x^d \pmod{n}$.

Parašo tikrinimas: parašas priimamas, jeigu $y^e \equiv x \pmod{n}$ arba jeigu x neatsiustas, įvertinus $y^e \pmod{n}$ pagal prasmę.

Aklas RSA parašas

B nori, kad A sukurtų galiojantį teksto m RSA parašą, bet nepamatytų paties teksto.

Tegu A raktai yra $K_{v,A} = \langle e_A, n_A \rangle$ ir $K_{p,A} = \langle d_A \rangle$. Parinkusi skaičių r , $(r, n) = 1$, B apskaičiuoja

$$x \equiv r^{e_A} m \pmod{n_A}$$

ir nusiunčia A pasirašyti.

A pasirašo ir atsiunčia B parašą

$$z = \text{sig}(x|K_{p,A}) \equiv x^{d_A} \pmod{n_A}.$$

Dabar B skaičiuoja

$$y \equiv r^{-1} z \equiv r^{-1} x^{d_A} \equiv r^{-1} (r^{e_A} m)^{d_A} \equiv m^{d_A} \pmod{n_A}.$$

Taigi $y = \text{sig}(m|K_{p,A})$ yra galiojantis teksto m parašas.

ElGamalio tipo skaitmeniniai parašai

ElGamalio skaitmeninis parašas

Pasirašomų tekstų aibė $\mathcal{M} = \mathbb{F}_p^*$, čia p – didelis pirminis skaičius; parašų aibė $\mathcal{P} = \mathbb{F}_p^* \times \mathbb{Z}_{p-1}$.

Privatusis raktas: $K_p = \langle a \rangle, a \in \mathbb{Z}_{p-1}$.

Viešasis raktas: $K_v = \langle p, \alpha, \beta \rangle$, čia α – generuojantis elementas, $\beta \equiv \alpha^a \pmod{p}$.

Parašo sudarymas: pasirenkamas atsitiktinis k , $(k, p-1) = 1$ ir skaičiuojama:

$$\gamma \equiv \alpha^k \pmod{p}, \delta \equiv (x - a\gamma)k^{-1} \pmod{p-1}, \\ \langle \gamma, \delta \rangle = \text{sig}(x|K_p).$$

Parašo tikrinimas: parašas priimamas tada ir tik tada, kai $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$.

ElGamalio skaitmeninio parašo saugumas

Jeigu du skirtingi pranešimai pasirašomi, panaudojus tą patį k , tai iš parašų

$$\text{sig}(x_1|K_p) = \langle \gamma, \delta_1 \rangle, \quad \text{sig}(x_2|K_p) = \langle \gamma, \delta_2 \rangle$$

galima surasti privatųjį raktą!

Schnorro skaitmeninis parašas

Pranešimų aibė $\mathcal{M} = \mathbb{F}_q$, čia q yra pirminis skaičiaus $p - 1$ daliklis; p irgi yra pirminis.

Privatusis raktas: $K_p = \langle a \rangle, 0 < a < q - 1$.

Viešasis raktas: $K_v = \langle p, q, \alpha, \beta \rangle$, $\alpha \in \mathbb{F}_p$ yra q -osios eilės elementas, $\beta \equiv \alpha^{-a} \pmod{p}$.

Parašo sudarymas: pasirašomas tekstas yra x ; parinkus skaičių $0 \leq r < q - 1$, skaičiuojama:

$$\gamma \equiv \alpha^r \pmod{p}, \delta \equiv r + ax \pmod{q}, \text{sig}(x|K_p) = \langle \gamma, \delta \rangle.$$

Parašo tikrinimas: pranešimo x parašas $\text{sig}(x|K_p) = \langle \gamma, \delta \rangle$ priimamas tada ir tik tada, kai $\alpha^\delta \beta^x \equiv \gamma \pmod{p}$.

DSA

Pranešimų aibė $\mathcal{M} = \mathbb{F}_p^*$, parašų aibė – $\mathcal{P} = \mathbb{F}_q \times \mathbb{F}_q$, čia q yra pirminis $p - 1$ daliklis.

Privatusis raktas: $K_p = \langle a \rangle$, $0 < a < q - 1$.

Viešasis raktas: $K_v = \langle p, q, \alpha, \beta \rangle$, $\alpha \in \mathbb{F}_p$ yra q -osios eilės elementas, $\beta \equiv \alpha^a \pmod{p}$.

Parašo sudarymas: pranešimui pasirašyti parenkamas skaičius $k \in \mathbb{F}_q^*$ ir skaičiuojama: $\text{sig}(x|K_p) = \langle \gamma, \delta \rangle$,

$$\gamma \equiv \alpha^k \pmod{p} \pmod{q}, \quad \delta \equiv (x + a\gamma)k^{-1} \pmod{q}.$$

Turi būti patenkinta sąlyga $(\delta, q) = 1$.

Parašo tikrinimas: parašas pripažįstamas tada ir tik tada, kai

$$\begin{aligned} \alpha^{e_1} \beta^{e_2} \pmod{p} &\equiv \gamma \pmod{q}, \\ e_1 &\equiv x\delta^{-1} \pmod{q}, e_2 \equiv \gamma\delta^{-1} \pmod{q}. \end{aligned}$$

Rabino skaitmeninis parašas

Raktai sudaromi kaip ir kriptosistemoje:

$$K_{pr} = \langle p, q \rangle, \quad K_v = \langle n \rangle, \quad p, q \equiv 3 \pmod{4}.$$

Pranešimų, kuriuos galima pasirašyti aibė: $\mathcal{M} = \{m^2 : m \in \mathbb{Z}_n\}$.

Parašo sudarymas: pranešimo $x \in \mathcal{M}$ parašas – lyginio $s^2 \equiv x \pmod{n}$ sprendinys.

Parašo tikrinimas: pranešimas $x \in \mathcal{M}$ parašas – s . Tikrinama, ar $s^2 \equiv x \pmod{n}$.

Nepaneigiamo parašo schema

D.Chaum ir H. van Antverpeno schema

Raktų sudarymas. p – didelis pirminis skaičius, q – pirminis $p - 1$ daliklis, o $\alpha \in \mathbb{Z}_p^*$ – q -os eilės elementas. Raktai:

$$K_p = \langle a \rangle, \quad K_v = \langle p, \alpha, \beta \rangle, \quad \beta \equiv \alpha^a \pmod{p}.$$

Parašo sudarymas. Pranešimų ir parašų aibė:

$$\mathcal{M} = \{\alpha^m : m = 0, \dots, q - 1\}.$$

Jei $x \in \mathcal{M}$, tai $\text{sig}(x|K_p) \equiv x^a \pmod{p}$.

Parašo tikrinimas

A turi patikrinti, ar y yra B parašas. Tikrinimo protokolas vykdomas taip:

- A parenka atsitiktinius skaičius $e_1, e_2 \in \mathbb{Z}_q^*$, skaičiuoja $c \equiv y^{e_1} \beta^{e_2} \pmod{p}$ ir siunčia B;
- B skaičiuoja $d \equiv c^{a^{-1} \pmod{q}} \pmod{p}$ ir siunčia A;
- parašas priimamas tada ir tik tada, kai

$$d \equiv x^{e_1} \alpha^{e_2} \pmod{p}.$$

Parašo tikrinimas

Jeigu parašas yra tikras, t.y. $y \equiv x^a \pmod{p}$, tai jis bus priimtas. Gali atsitikti, kad bus už teisingą priimtas ir negaliojantis parašas.

Teorema. Jei $y \not\equiv x^a \pmod{p}$, tai tikimybė, kad y bus pripažintas pranešimo x parašu lygi $1/q$.

Parašo tikrinimas

Parašo tikrinimo protokolas gali duoti neigiamą atsakymą dviem atvejais:

- kai parašas iš tikrųjų netikras, t.y. $y \not\equiv x^a \pmod{p}$
- kai B nesilaiko protokolo.

Parašo tikrinimas

Jeigu tikrinimo protokolas duoda neigiamą atsakymą, protokolas dar kartą kartojamas:

- A parenka atsitiktinius skaičius $f_1, f_2 \in \mathbb{Z}_q^*$, skaičiuoja $C \equiv y^{f_1} \beta^{f_2} \pmod{p}$ ir siunčia B;
- B skaičiuoja $D \equiv C^{a^{-1} \pmod{q}} \pmod{p}$ (arba pasirenka D „nuo lubų“) ir siunčia A;
- jeigu $D \equiv x^{f_1} \alpha^{f_2} \pmod{p}$, A parašą pripažįsta;
- jeigu $D \not\equiv x^{f_1} \alpha^{f_2} \pmod{p}$ A laiko parašą klastote tada ir tik tada, kai $(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} \pmod{p}$, priešingu atveju A apkaltina B protokolo nesilaikymu.

Parašo tikrinimas

Teorema. Jei $y \equiv x^a \pmod{p}$, tačiau ir A, ir B laikosi protokolo, tai

$$(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} \pmod{p}.$$

Teorema. Jei $y \equiv x^a \pmod{p}$, ir B parenka d, D , kad

$$d \not\equiv x^{e_1} \alpha^{e_2} \pmod{p}, \quad D \not\equiv x^{f_1} \alpha^{f_2} \pmod{p},$$

tai tikimybė, kad $(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} \pmod{p}$. lygi $1/q$.

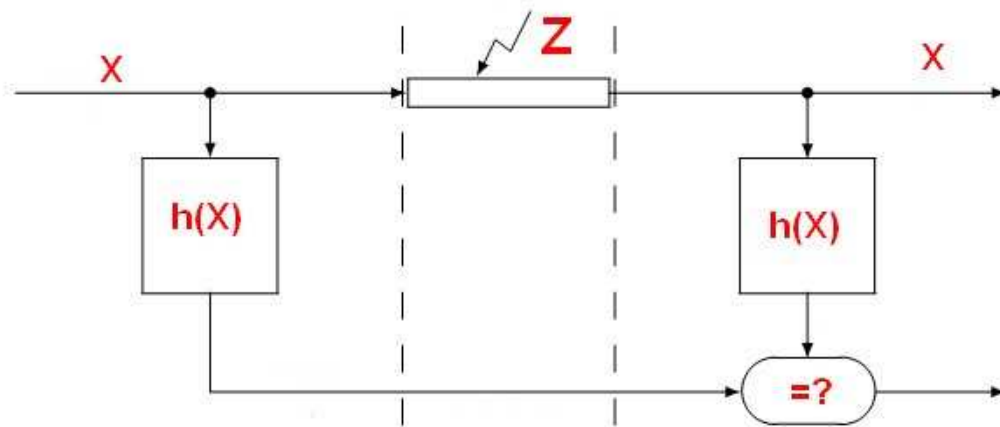
Kriptografinės maišos funkcijos

Maišos funkcijos

Maišos funkcijos sukuria dokumentų santraukas (digest).

Taikymas – duomenų paieškos organizavimui.

Kriptografinių maišos funkcijų paskirtis



Maišos funkcijos (hash functions, message digest, fingerprint, cyclical redundancy check (CRC), manipulation detection codes (MDC))

Publikacija neatskleidžiant turinio

M – tekstas, R – atsitiktinai generuotas žodis.
Galima paskelbti

$$H = h(M||R).$$

Sutapimai ir maišos funkcijos

Apibrėžimas. Tegu $h : \mathcal{M} \rightarrow \mathcal{H}$ yra maišos funkcija. Jeigu $x, x^* \in \mathcal{M}, x \neq x^*$, bet $h(x) = h(x^*)$, tai šią porą vadinsime sutapimo pora, arba tiesiog sutapimu (collision, angl.). Funkciją vadinsime **atsparia sutapimams**, jeigu nėra efektyvaus algoritmo duotajam $x \in \mathcal{M}$, randančio $x^* \in \mathcal{M}, x^* \neq x$, kad $h(x) = h(x^*)$.

Funkciją vadinsime **labai atsparia sutapimams**, jeigu nėra efektyvaus algoritmo, randančio kokią nors sutapimų porą.

Iteracijų seka

Tarkime, turime tam tikrą funkciją

$$C : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n. \quad (3)$$

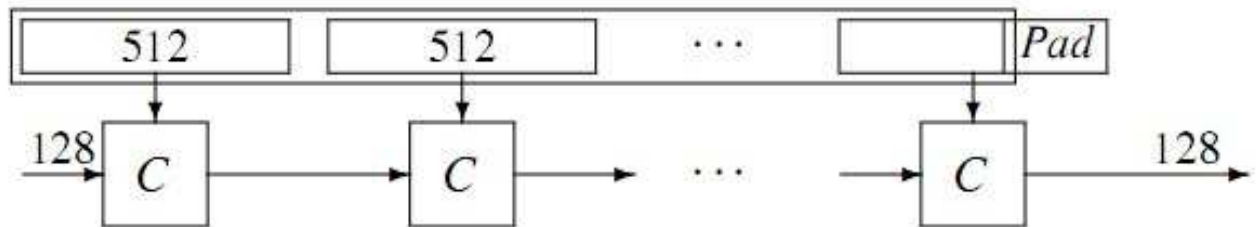
Tada, panaudoję ją, galime sukonstruoti maišos funkciją $h : \{0, 1\}^* \rightarrow \mathcal{C}, \mathcal{C} = \{0, 1\}^n$. Bet kokio ilgio tekstą $x \in \{0, 1\}^*$ padalykime n ilgio žodžiais, jeigu reikia, papildydami paskutinįjį žodį iki reikiamo ilgio:

$$x = x_1 x_2 \dots x_t, \quad x_i \in \{0, 1\}^n.$$

Tegu $h_0 \in \{0, 1\}^n$ yra koks nors pradinis fiksuotas žodis. Apibrėžkime

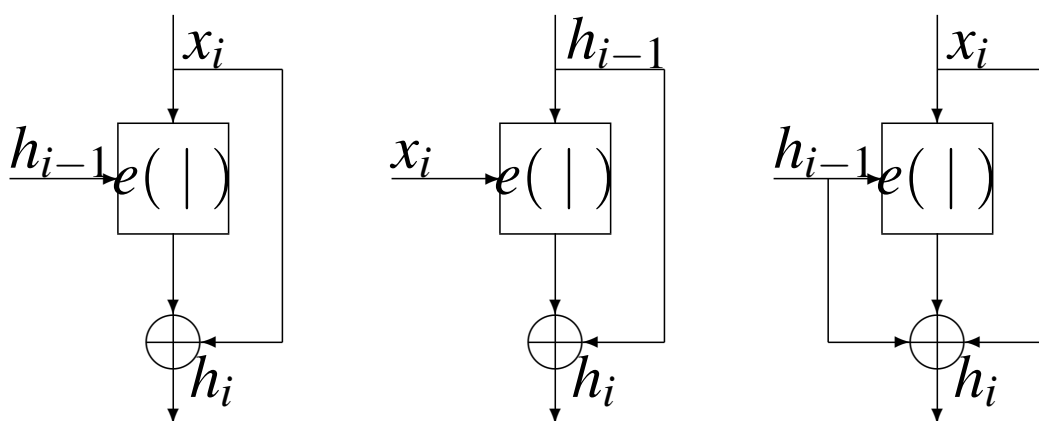
$$h_i = C(h_{i-1}, x_i), \quad i = 1, 2, \dots, t, \quad h(x) = h_t.$$

Merkle-Damgaard schema



Teorema. Jeigu C yra atspari sutapimams, tai ir maišos funkcija yra atspari sutapimams.

Maišos funkcijos iš blokinių kriptosistemų



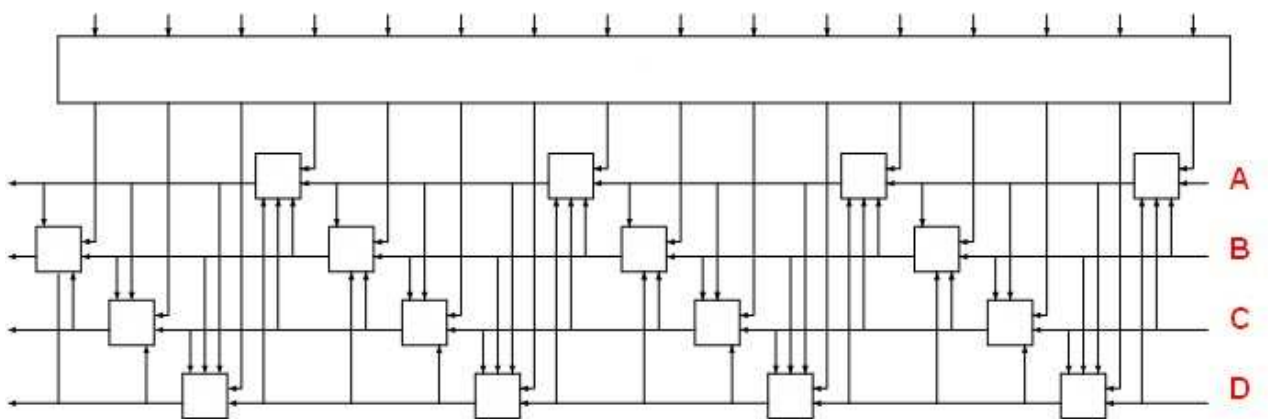
Matyaso-Meyerio-Oseaso, Davieso-Meyerio ir Miyaguchi-Preneelio metodai maišos funkcijoms konstruoti iš blokinių kriptosistemų.

Dažniausiai naudojamos maišos funkcijos

- **MD4** 128 bitai
- **MD5** 128 bitai
- **SHA-1** 160 bitų
- **RIPEDM-160** 160 bitų
- **SHA-256, SHA-384, SHA-512**

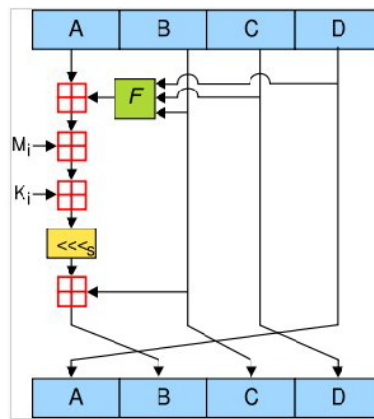
MD5

R. Rivest (1991), Interneto standartas RFC
1321 (1992)



Bloko ilgis – 512 bitų, santrauka – 128 bitai,
atliekamos 4 iteracijos.

Viena MD5 dėžė



$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z),$$

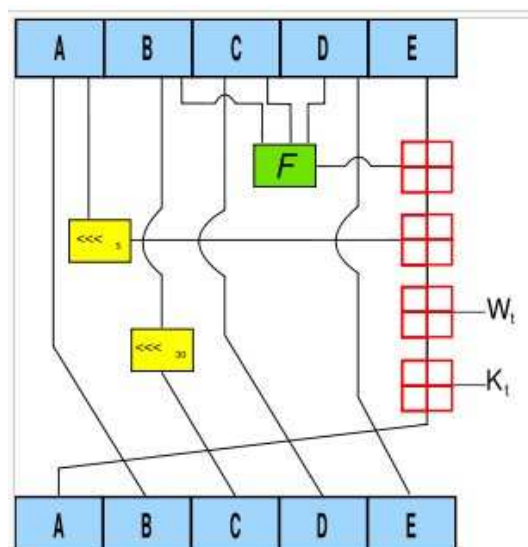
$$G(X, Y, Z) = (X \wedge Y) \vee (X \wedge \neg Z),$$

$$H(X, Y, Z) = X \oplus Y \oplus Z,$$

$$H(X, Y, Z) = Y \oplus (X \vee \neg Z).$$

SHA

SHA – FIPS standartas (1993). Variantai: SHA-160, SHA-224, SHA-256, SHA-384, SHA-512. Bloko ilgis – 512.



Viena iteracija: A, B, C, D, E – 32 bitų žodžiai,

Iteracijos konstantos

Prieš pradedant darbą registrai užpildomi pradinėmis standartinėmis reikšmėmis. Pirmasis teksto 512 bitų ilgio blokas padalijamas į 16 žodžių po 32 bitus: $m[0], m[1], \dots, m[15]$. Su šiuo bloku bus atliekama 80 operacijų, kiekvienai operacijai reikalinga 32 bitų žodžių pora K_t, W_t , $t = 0, 1, \dots, 79$. Jos sudaromos taip:

$$K_t = \begin{cases} \left\lfloor 2^{30} \sqrt{2} \right\rfloor, & 0 \leq t \leq 19, \\ \left\lfloor 2^{30} \sqrt{3} \right\rfloor, & 20 \leq t \leq 39, \\ \left\lfloor 2^{30} \sqrt{5} \right\rfloor, & 40 \leq t \leq 59, \\ \left\lfloor 2^{30} \sqrt{10} \right\rfloor, & 60 \leq t \leq 79, \end{cases}$$

$$W_t = \begin{cases} m[t], & 0 \leq t \leq 15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \leftarrow 1, & 15 < t < 80, \end{cases}$$

SHA iteracijų funkcijos

$$f_t(x, y, z) = \begin{cases} (x \wedge y) \vee ((\neg x) \wedge z), & 0 \leq t \leq 19, \\ x \oplus y \oplus z, & 20 \leq t \leq 39, \\ (x \wedge y) \vee (x \wedge z) \vee (y \wedge z), & 40 \leq t \leq 59, \\ x \oplus y \oplus z, & 60 \leq t \leq 79. \end{cases}$$

SHA

kiekviename žingsnyje $t = 0, 1, \dots, 79$ atliekami tokie veiksmi:

$$T = (A \leftarrow 5) + f_t(B, C, D) + E + W_t + K_t,$$

$$E = D,$$

$$D = C,$$

$$C = B \leftarrow 30,$$

$$B = A,$$

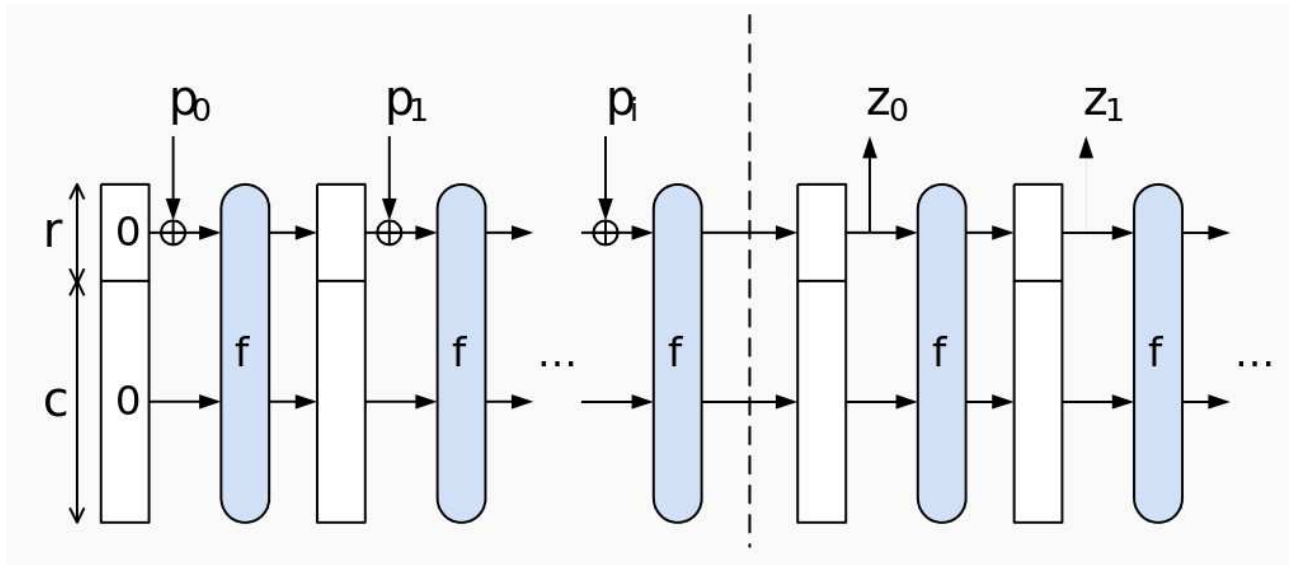
$$A = T.$$

Naujas konkursas

The screenshot shows the NIST Computer Security Division (CSRC) website. The header includes the NIST logo, the text "National Institute of Standards and Technology Information Technology Laboratory", a search bar, and navigation links: ABOUT, MISSION, CONTACT, STAFF, SITE MAP. Below the header, the main navigation bar includes CSRC HOME, GROUPS, PUBLICATIONS, DRIVERS, NEWS & EVENTS, and ARCHIVE. The main content area is titled "CRYPTOGRAPHIC HASH ALGORITHM COMPETITION". The text states: "NIST has opened a public competition to develop a new cryptographic hash algorithm, which converts a variable length message into a short 'message digest' that can be used for digital signatures, message authentication and other applications. The competition is NIST's response to recent advances in the cryptanalysis of hash functions. The new hash algorithm will be called 'SHA-3' and will augment the hash algorithms currently specified in FIPS 180-2, Secure Hash Standard. Entries for the competition must be received by **October 31, 2008**. The competition is announced in the [Federal Register Notice published on November 2, 2007](#); further details of the competition will be available at the specific sites indicated in the menu on the left." A sidebar on the left lists links: Cryptographic Hash Project, Cryptographic Hash Algorithm Competition (selected), Timeline for Hash Algorithm Competition, Federal Register Notices, Submission Requirements, Public Comments, Email Mailing List, Contacts, and Other Links. The footer includes the NIST logo, a disclaimer: "Hash Project Webmaster, Disclaimer Notice & Privacy Policy", "NIST is an Agency of the U.S. Department of Commerce", and update information: "Last updated: January 23, 2008" and "Page created: April 15, 2005".

14 kandidatų atrinkta antrajam raundui.

Laimėtoja: Keccak maišos funkcija



„Kempinės“ schema

„Gimtadienio“ ataka

Pasirinkime skirtingus x_1, x_2, \dots, x_n ir apskaičiuokime $z_1 = h(x_1), z_2 = h(x_2), \dots, z_n = h(x_n)$. Jeigu nors dvi reikšmės sutapo, sutapimas rastas.

Tegu iš viso santraukų yra m , t. y. $|\mathcal{H}| = m$.

Lengviau suskaičiuoti tikimybę q , kad santraukos bus skirtingos

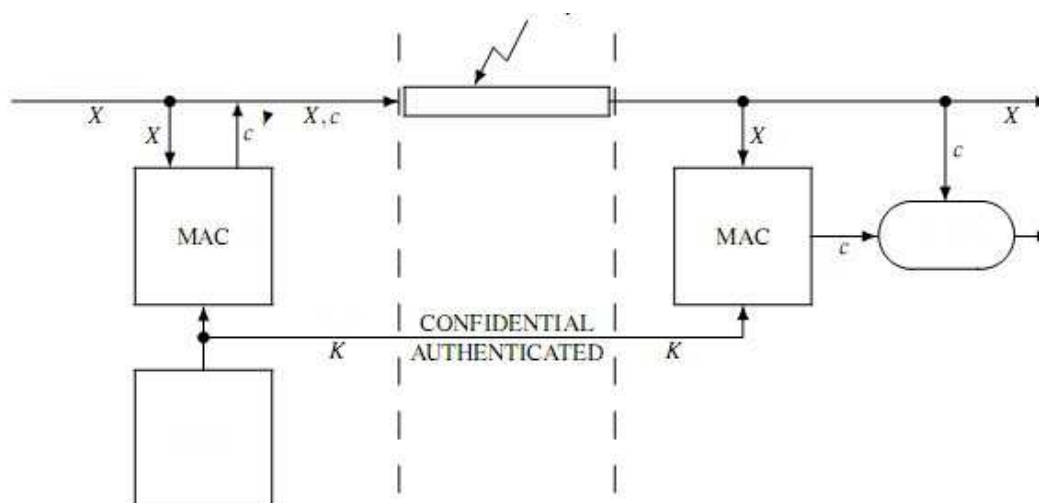
„Gimtadienio“ ataka

$$q = \frac{m(m-1)\dots(m-n+1)}{m^n} = \left(1 - \frac{1}{m}\right) \left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{n-1}{m}\right)$$
$$\approx \exp\left\{-\frac{1}{m} \sum_{i=1}^{n-1} i\right\} \approx \exp\left\{-\frac{1}{2m} n^2\right\}.$$

Jeigu sutapimo radimo tikimybė šiuo metodu yra ε , tai $q = 1 - \varepsilon$ ir

$$m \approx \frac{-n^2}{2\ln(1 - \varepsilon)}.$$

MAC



MAC iš maišos funkcijų

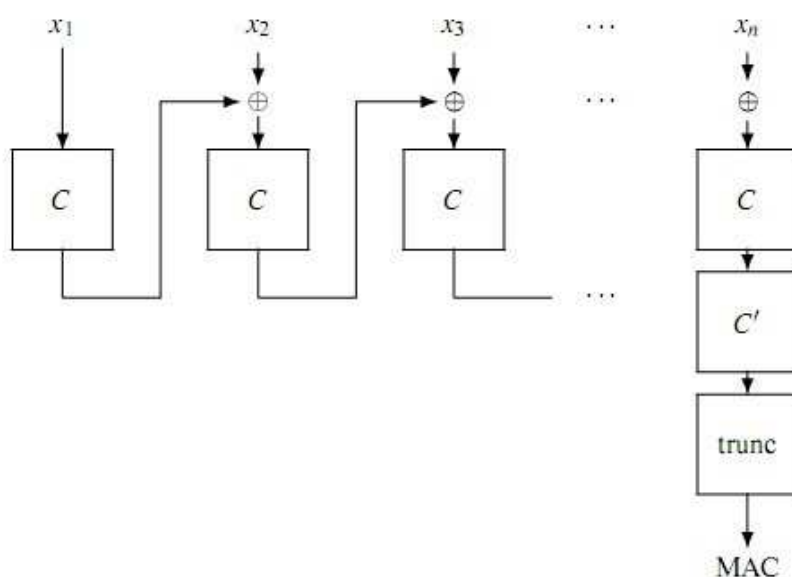
Jei h yra maišos funkcija, galima konstruoti:

$$MAC(X|k) = h(k||X), \text{ arba } MAC(X|k) = h(X||k).$$

Abu būdai nesaugūs! Gudresnis būdas

$$HMAC(X|k) = h(k||p_1||h(k||p_2||X))$$

Blokiniai šifrai ir MAC



$$h = MAC(X|k) \text{ su šifravimu } e(X|k_1)||MAC(e(X|k_1)|k_2)$$

Reikalingas susitarimas kaip užbaigti nepilnus blokus!

Jeigu nebūtų pabaigos žingsnio

Jeigu paskutinės iteracijos bloką laikytume MAC reikšme:

$$\begin{aligned} X &= x_1 || x_2 || \dots || x_t, \quad M = \text{MAC}(X || k), \\ Y &= X || M \oplus x_1 || X^*, \quad M = \text{MAC}(Y || k), \quad X^* = x_2 || \dots || x_t. \end{aligned}$$

Paslapties dalijimo schemas

Visi turi dalyvauti!

Paslaptis – ilgas dvejetainės abėcėlės žodis $S \in \{0, 1\}^m$, o padalyti paslaptį reikia taip, kad tik visi dalyviai susirinkę galėtų ją atkurti.

Dalytojas atsitiktinai parenka $n - 1$ -ą žodį

$S_1, \dots, S_{n-1} \in \{0, 1\}^m$ ir apskaičiuoja

$$S_n = S \oplus S_1 \oplus S_2 \oplus \dots \oplus S_{n-1}.$$

D_i gauna savo paslapties dalį S_i .

Susirinkę visi kartu gali atkurti paslaptį taip:

$$S = S_1 \oplus S_2 \oplus \dots \oplus S_{n-1} \oplus S_n.$$

Shamiro schema

m yra didelis natūrinis skaičius, o paslaptis – koks nors skaičius $S \in \mathbb{Z}_m$.

Dalytojas D atsitiktinai parenka skaičius $S_1, S_2, \dots, S_{n-1} \in \mathbb{Z}_m$ ir apskaičiuoja

$$S_n \equiv S - S_1 - S_2 - \dots - S_{n-1} \pmod{m}.$$

Dalyvis D_i gauna savo paslapties dalį S_i . Jas visas sudėjus gaunama tikroji paslaptis:

$$S \equiv S_1 + S_2 + \dots + S_n \pmod{m}.$$

Schema su slenksčiu

Apibrėžimas. Tegu S yra paslaptis, o S_1, S_2, \dots, S_n yra jos dalys, kurias dalytojas D įteikė dalyviams D_1, D_2, \dots, D_n . Ši paslapties padalijimą vadinsime paslapties dalybomis su slenksčiu t ($1 \leq t \leq n$), jeigu S galima atkurti tik iš ne mažiau kaip t bet kurių paslapties dalių.

Shamiro schema

Dalytojas D parenka pakankamai didelį pirminį skaičių p , $p > n$, parenka skirtingus skaičius $x_1, x_2, \dots, x_n \in \mathbb{F}_p$ ir kiekvienam dalyviui D_i įteikia x_i .

Šie skaičiai nėra slapti. Paslaptis yra skaičius $S \in \mathbb{F}_p$.

Dalytojas atsitiktinai pasirenka skaičius a_1, a_2, \dots, a_{t-1} ir sudaro daugianarį

$$a(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \in \mathbb{F}_p[x].$$

Paslapties dalis, kuri įteikiama dalyviui D_i , yra $S_i \equiv a(x_i) \pmod{p}$.

Shamiro schema

Paslaptį S , t. y. laisvąjį daugianario narį, galima nustatyti iš bet kurių t paslapties dalių $S_{i_1}, S_{i_2}, \dots, S_{i_t}$:

$$S + a_1x_{i_1} + a_2x_{i_1}^2 + \dots + a_{t-1}x_{i_1}^{t-1} = S_{i_1},$$

$$S + a_1x_{i_2} + a_2x_{i_2}^2 + \dots + a_{t-1}x_{i_2}^{t-1} = S_{i_2},$$

.....

$$S + a_1x_{i_t} + a_2x_{i_t}^2 + \dots + a_{t-1}x_{i_t}^{t-1} = S_{i_t}$$

Shamiro schema

Paslapties dalijimas: D – dalytojas, D_1, D_2, \dots, D_n – dalyviai.

D parenka pirminį p , skirtingus $x_1, x_2, \dots, x_n \in \mathbb{F}_p$ ir D_i įteikia skaičių x_i . Pirminis p yra viešas, paslaptis – skaičius $S \in \mathbb{F}_p$.

D parenka skaičius a_1, a_2, \dots, a_{t-1} , sudaro daugianarį

$$a(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$

ir paslapties dalis $S_i \equiv a(x_i) \pmod{p}$, įteikia jas D_i .

Paslapties atkūrimas: susirinkę t dalyvių $D_{i_1}, D_{i_2}, \dots, D_{i_t}$ paslaptį gali atkurti taip:

$$S \equiv \sum_{i=1}^t S_{i_j} \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \pmod{p}.$$

Blakely schema

p didelis pirminis skaičius, paslaptis – skaičius $S < p$. Dalytojas parenka skaičius s_2, s_3, \dots, s_t , sudaro $\mathbf{s} = \langle s_1, s_2, \dots, s_t \rangle$, $s_1 = S$. Dalyvio D_j paslapties dalis: parenka atsitiktinius elementus $a_1^{(j)}, a_2^{(j)}, \dots, a_{t-1}^{(j)}$, apskaičiuoja

$$c_j \equiv s_t - \sum_{i=1}^{t-1} a_i^{(j)} s_i \pmod{p}$$

ir įteikia dalyviui D_j lygtį

$$x_t \equiv c_j + \sum_{i=1}^{t-1} a_i^{(j)} x_i \pmod{p}.$$

Susirinkę t dalyvių gali sudaryti t lygčių su t nežinomųjų sistemą ir ją išsprendę rasti paslaptį $m_1 = S$.

Karnino-Greeno-Hellmano schema

Paslapties dalijimui naudojama kokia nors m -matė erdvė \mathbb{F}^m . Jeigu dalyvių yra n , tai dalytojas parenka $V_1, V_2, \dots, V_n \in \mathbb{F}^m$, kad bet kurie m šios sistemos vektoriai sudarytų \mathbb{F}^m bazę.

Prenkami dar du vektoriai: $V_0, U \in \mathbb{F}^m$, paslaptis yra skaičius $S = V_0 \cdot U$ (skaljarinė sandauga).

Vektoriai V_i gali būti paskelbti viešai, dalyviui įteikiama paslapties dalis yra skaičius $S_i = V_i \cdot U$.

Bet kurie m dalyviai gali surasti U ir atkurti paslaptį S .

Asmutho-Bloomo schema

Paslapties dalijimas: dalytojas D parenka skaičius

$$\begin{aligned}p &< p_1 < p_2 < \dots < p_n, \quad (p_i, p_j) = 1, \quad i \neq j, \\N &= p_1 p_2 \dots p_t, \quad N^* = p_n p_{n-1} \dots p_{n-t+2} \\N &> N^*.\end{aligned}$$

Paslaptis – skaičius $S, S < p$.

Dalytojas parenka $r, N^*/p < r < N/p - 1$, apskaičiuoja $S^* = S + rp$. Dalyviui D_i paskiriamas skaičius p_i ir saugiu kanalu perduodama paslapties dalis $S_i \equiv S^* \pmod{p_i}$.

Asmutho-Bloomo schema

Paslapties atkūrimas: t dalyvių, naudodamiesi kiniškąja liekanų teorema išsprendžia lyginių sistemą

$$x \equiv S_{i_j} \pmod{p_{i_j}} \quad (j = 1, 2, \dots, t)$$

ir randa sprendinį $x \equiv S^* \pmod{p_{i_1} \dots p_{i_t}}$. Paslaptis $S \equiv S^* \pmod{p}$.

Leidimų struktūros

Apibrėžimas. Tegu $\mathbf{D} = \{D_1, D_2, \dots, D_n\}$ yra dalyvių aibė. Jos poaibių sistemą \mathcal{G} vadinsime leidimų struktūra, jeigu kiekvienos aibės $A \subset \mathcal{G}$ viršaibis B (t. y. aibė, tenkinanti sąlygą $A \subset B$) taip pat įeina į \mathcal{G} .

Apibrėžiant leidimų struktūrą \mathcal{G} , pakanka nurodyti tik tokia jos posistemę $\Gamma \subset \mathcal{G}$, kad su kiekviena $A \in \Gamma$ jos poaibiai nepriklausytų Γ . Tokią posistemę vadinsime leidimų struktūros branduoliu.

Paslapties dalijimas pagal leidimų struktūrą

Apibrėžimas. Sakysime, kad paslapties padalijimo schema realizuoja leidimų struktūrą \mathcal{G} , jeigu paslaptį iš savo dalių gali atkurti tik tokie dalyviai, iš kurių sudarytas poaibis priklauso \mathcal{G} .

Realizuojant leidimų struktūrą \mathcal{G} , reikia paslaptį padalyti taip, kad ją galėtų atkurti poaibių iš branduolio Γ dalyviai, tačiau negalėtų atkurti tokie dalyviai, kurie nesudaro jokio B iš Γ viršaibio.

Benaloho-Leichterio metodas

$\mathbf{D} = \{D_1, D_2, D_3, D_4, D_5\}$ yra dalyvių aibė,

$$G_1 = \{D_1, D_4, D_5\}, G_2 = \{D_1, D_2, D_4\}, G_3 = \{D_3, D_4\}$$

leidimų struktūros branduolys. Leidimų struktūrą galima realizuoti kiekvienai branduolio grupei dalijant paslaptį pagal Shamiro schemą.

Brickelio schema

Dalyvių aibė yra $\mathbf{D} = \{D_1, D_2, \dots, D_n\}$, o Γ – leidimų struktūros, kurią reikia realizuoti, branduolys. Paslaptis yra skaičius S .

Dalytojas turi parinkti pakankamai didelį pirminį skaičių p , natūrinį skaičių d ir sukonstruoti funkciją $\delta : \mathbf{D} \rightarrow \mathbb{F}_p^d$, tenkinančią tokią sąlygą:

$$\langle 1, 0, \dots, 0 \rangle \in \mathcal{L}(\delta(D_{i_1}), \delta(D_{i_2}), \dots, \delta(D_{i_r}))$$

tada ir tik tada, kai dalyvių aibė $\{D_{i_1}, D_{i_2}, \dots, D_{i_r}\}$ yra kokios nors aibės iš branduolio viršaišis. Ši funkcija gali būti vieša.

Brickelio schema

Dalytojas, parinkęs $a_2, a_3, \dots, a_d \in \mathbb{F}_p$ atsitiktinai, sudaro dar vieną vektorių

$$\mathbf{a} = \langle a_1, a_2, \dots, a_d \rangle, \quad a_1 = S,$$

ir apskaičiuoja paslapties dalis $S_i \equiv \mathbf{a} \cdot \delta(D_i) \pmod{p}$.

Brickelio schema

Susirinko dalyviai, kurių sudaroma aibė G priklauso leidimų struktūros branduoliui arba yra jo viršaišis. Išsprendę tiesinių lygčių sistemą, jie gali surasti skaičius c_i , kad būtų

$$\langle 1, 0, \dots, 0 \rangle = \sum_{D_i \in G} c_i \delta(D_i).$$

Jeigu padauginsime skaliariškai šią lygybę iš \mathbf{a} , gausime

$$\langle S, 0, \dots, 0 \rangle \equiv \sum_{D_i \in G} c_i (\mathbf{a} \cdot \delta(D_i)) \equiv \sum_{D_i \in G} c_i S_i \pmod{p}.$$

Įvairūs sukčiavimai

- Jeigu susirinko tiek dalyvių kiek reikia, o bent vienas jų parodė neteisingą savąją dalį - paslaptis nebus atkurta;
- jeigu susirinko tiek dalyvių, kiek reikia, bet vienas jų - Zigmas, apsimetęs teisėtu dalyviu, jis sužinos kitų dalyvių dalis.
- jeigu susirinko t teisėtų dalyvių ir $t - 1$ iš jų nusprendė apgauti paskutinįjį: atkurti paslaptį gavus iš paskutiniojo jo paslapties dalį, bet nurodžius jam savo dalis neteisingai - jiems pavyks.
-

Sukčiavimo ženklas

Shamiro paslapties padalijimo schema su (t, n) slenksčiu ir paslaptimi – skaičiumi $k \in \{1, 2, \dots, s - 1\}$.

Prenkamas modulis – pirminis skaičius

$$p > \max((s - 1)(t - 1)/\varepsilon + t, n).$$

Dalyvis gauna dalį

$$\langle x_i, y_i = a(x_i) \rangle, \quad x_i \in \mathbb{Z}_p.$$

Skaičiai x_i yra skirtingi ir parinkti atsitiktinai.

Jeigu atkuriant paslaptį gaunamas skaičius $k > s$, konstatuojama apgavystė.

Tikimybė, kad $t - 1$ dalyvis apgaus paskutinįjį yra ne didesnė už ε .

Schema su užmaskuotomis paslapties dalimis

Du pirminiai skaičiai: p, q , $q|p-1$, $q \geq n+1$, čia n yra dalyvių skaičius, t - schemos slenksčio parametras.

Dalytojas pasirenka daugianarį

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \in \mathbb{Z}_q[x].$$

Kiekvienam dalyviui atiduoda $x_i \in \mathbb{Z}_q$ ir $y_i = f(x_i)$, čia x_i yra viešas parametras, o y_i – paslapties dalis.

Schema su užmaskuotomis paslapties dalimis

Tegu $g \in \mathbb{Z}_p$ yra q -osios eilės elementas. Paslaptis yra

$$k \equiv g^{a_0} \equiv g^{f(0)} \pmod{p}.$$

Kiekvienas dalyvis apskaičiuoja „užmaskuotą“ paslapties dalį

$$z_i \equiv g^{y_i} \pmod{p}.$$

Paslaptį k galima atkurti iš t užmaskuotų dalių:

$$k \equiv \prod_{j=1}^t z_j^{b_j} \pmod{p}, \quad b_j \equiv \prod_{k, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \pmod{q}.$$

Schema su užmaskuotomis paslapties dalimis

Šios schemos savybė - galima generuoti naują paslapties padalijimo variantą, neperdalijant paslapties.

Parinkus atsitiktinį skaičių r skaičiuojamas ir paskelbiamas naujas generuojantis elementas $\bar{g} \equiv g^r \pmod{p}$ ir dalyviai susiskaičiuoja naujas „užmaskuotas“ dalis $\bar{g}^{y_i} \pmod{p}$ naujai paslapčiai $k^* \equiv k^r \pmod{p}$ atkurti.

ElGamalio šifras dalyvių grupei

Raktų sudarymas ir padalijimas. Dalyvių skaičius n , slenksčio dydis t .

Pirminiai skaičiai p, q , skaičius $q, q > n$, dalija $p - 1$. Dalintojas parenka q -osios eilės elementą $g \in \mathbb{Z}_p$, paslaptį $a \in \mathbb{Z}_q$, skaičiuoja $y \equiv g^a \pmod{p}$ ir skelbia viešąjį raktą

$$K_v = \langle p, q, g, y \rangle.$$

Dalintojas padalija paslaptį k dalyviams pagal Shamiro schemą su slenksčiu t ; t. y. i -ajam dalyviui įteikia skaičius $x_i, y_i \equiv a(x_i) \pmod{q}$.

ElGamalio šifras dalyvių grupei

Šifravimas. Pranešimas paverčiamas q -osios eilės elementu $M \in \mathbb{Z}_p$; parenkamas atsitiktinis $r \in \mathbb{Z}_q$ ir visiems dalyviams siunčiamas šifras

$$C = \langle C_1, C_2 \rangle = \langle g^r, My^r \rangle.$$

ElGamalio šifras dalyvių grupei

Dešifravimas. Dalyviai pateikia dešifravimui savo skaičius


$$x_i, z_i \equiv C_1^{y_i} \pmod{p}, \quad i = 1, 2, \dots, t.$$

Dešifravimo skaičiavimai


$$b_j \equiv \prod_{\substack{i=1, \dots, t \\ i \neq j}} x_i (x_i - x_j)^{-1} \pmod{q},$$

$$z \equiv \prod_{j=1}^t z_j^{b_j} \pmod{p},$$

$$M \equiv C_2 z^{-1} \pmod{p}.$$



Netiesioginiai įrodymai (ZKP zero-knowledge proofs)



Netiesioginiai įrodymai (ZKP zero-knowledge proofs)

Kam tokie įrodymai reikalingi?

Keblumas: kaip įsitikinti, kad interaktyvaus protokolo dalyvis elgiasi teisingai?

Pareikalauti, kad atskleistų naudotus dydžius negalime!

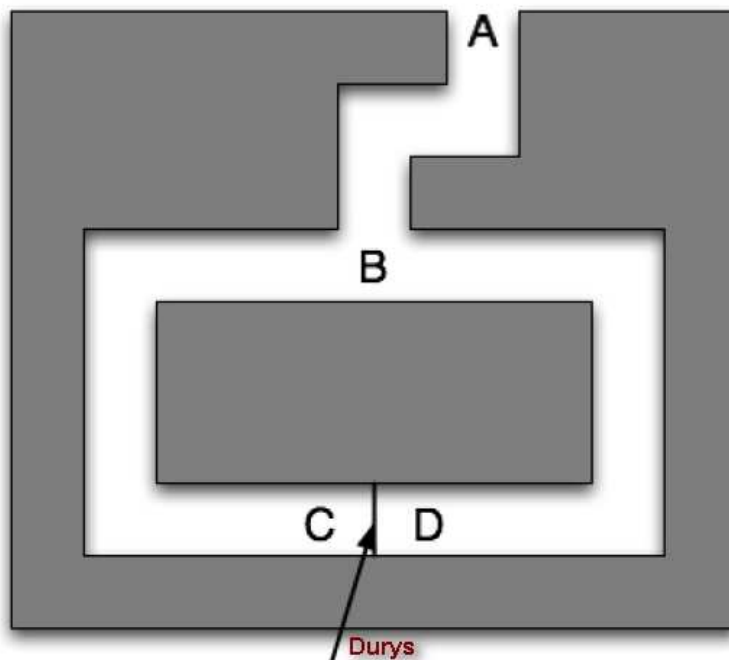
ZKP sąvoka

Dalyviai: įrodinėtoja I (Irena), tikrintojas T (Tomas).

I žino paslaptį ir nori tai įrodyti T, nesuteikdama jokių papildomų žinių.

ZKP - įrodymo protokolas, kuris nesuteikia tikrintojui jokių papildomų žinių.

Netiesioginio įrodymo galimybė



Reikalavimai įrodymui

Įrodymo schema

- Pilnumas: teisingas įrodymas visada pripažįstamas.
- Teisingumas: neteisingi įrodymai yra atmetami su didele tikimybe.

Grafų neizomorfiškumas

Irenos teiginys: Grafai G_1 ir G_2 yra neizomorfiški.

Interaktyvaus įrodymo eiga:

1. Tikrintojas skaičiuoja $H = \pi(G_i)$ ir siunčia Irenai.
2. Irena randa i ir siunčia Tikrintojui.

Protokolas kartojamas k kartų.

Grafų izomorfiškumo įrodymas

Irenos teiginys: G_1 ir G_2 yra izomorfiški; žinau π , $G_2 = \pi(G_1)$.

Įrodymo žingsniai:

- Irena sudaro $H = \sigma(G_1)$ ir siunčia T;
- T pasirenka $i = 1$ arba $i = 2$ ir siunčia I;
- Jei $i = 1$, I siunčia $\lambda = \sigma$. Jei $i = 2$, siunčia $\lambda = \sigma \circ \pi^{-1}$
- T tikrina ar $H = \lambda(G_i)$.

Protokolo vykdymo duomenis galima modeliuoti nedalyvaujant protokole!

Kas vyresnis?

Kaip A ir B gali interaktyviu protokolu nustatyti, kuris vyresnis neatskleisdami savo amžiaus?

B nori sužinoti, ar ji vyresnė Įrankis A viešojo rakto sistema, e_A šifravimo, d_A dešifravimo algoritmai. A skaičius (amžius) i , B skaičius j , abu skaičiai ne didesni už N .

Kas vyresnis?

Supaprastintas protokolas

- B pasirenka atsitiktinį x ir siunčia A skaičių $s = e_A(x) - j$;
- A skaičiuoja $y_u = d_A(s + u)$, $u = 1, 2, \dots, N$.
- A siunčia B skaičius

$$\langle y_1, y_2, \dots, y_i + 1, y_{i+1} + 1, \dots, y_N + 1 \rangle$$

- B tikrina, ar $y_j = x$. Jeigu taip, tai $i \geq j$.

Grafo spalvinimo uždavinys

Ar naudojant k spalvų duotojo grafo viršūnes galima nuspalvinti taip, kad kiekviena briauna jungtų skirtingomis spalvomis nuspalvintas viršūnes?

I teigia, kad grafą G galima nuspalvinti, nori tai įrodyti neatskleisdama paties spalvinimo.

Grafo spalvinimo uždavinys

Įrankis – kriptosistema. I nuspalvina grafą G .

- I pritaiko spalvų rinkiniui keitinį ir naujai nuspalvinto grafo kiekvienos viršūnės spalvą užšifruoja atskiru raktu: $y_i = e(sp_i | k_i)$.
- I pasiunčia T grafo viršūnių ir jų spalvų šifrų lentelę.
- T parenka dvi gretimas viršūnes ir pareikalauja jų šifrų raktų.
- I atsiunčia raktus ir T patikrina, ar tikrai viršūnės nuspalvintos skirtingai.

Kvadratinio lyginio sprendinys

I teiginys: žinau lyginio $x^2 \equiv c \pmod{n}$, čia $n = pq$, sprendinį u .

Įrodymo protokolas:

- I parenka atsitiktinį r ir siunčia $T \ y \equiv r^2 \pmod{n}$
- T parenka atsitiktinį $i \in \{0, 1\}$ ir siunčia I .
- I skaičiuoja $z \equiv u^i r \pmod{n}$ ir siunčia T .
- T tikrina, ar $z^2 \equiv c^i y \pmod{n}$

Protokolas kartojamas.

Gouillou-Quisquater schema

I teiginys: žinau lyginio $x^e \equiv c \pmod{n}$, čia $n = pq$, sprendinį u .

Įrodymo protokolas:

- I parenka atsitiktinį r ir siunčia $T \ y \equiv r^e \pmod{n}$
- T parenka atsitiktinį $i \in \{0, 1, \dots, e-1\}$ ir siunčia I .
- I skaičiuoja $z \equiv u^i r \pmod{n}$ ir siunčia T .
- T tikrina, ar $z^e \equiv c^i y \pmod{n}$

Protokolas kartojamas.

Diskretaus logaritmo žinojimo įrodymas

Viešos žinios: pirminis skaičius p , generuojantis elementas g ir y .

Irenos žinios: žino x , su kuriuo $y \equiv g^x \pmod{p}$.

Įrodymo protokolas:

- I renka atsitiktinį r , skaičiuoja $t \equiv g^r \pmod{p}$ ir siunčia T.
- T renka atsitiktinį c ir siunčia I;
- I skaičiuoja $s \equiv r + cx \pmod{(p-1)}$ ir siunčia T;
- T tikrina, ar $g^s \equiv ty^c \pmod{p}$.

Priklausomybės grupei įrodymas

Priklausymo grupei įrodymas:

Viešos žinios: n , $g \in \mathbb{Z}_n^*$, $g^q \equiv 1 \pmod{n}$, $y \in \mathbb{Z}_n^*$;

Irenos žinios: x , $0 \leq x \leq q-1$, $y \equiv g^x \pmod{p}$.

Įrodymo eiga:

- Irena pasirenka $0 \leq j \leq q-1$, skaičiuoja $\gamma \equiv g^j \pmod{n}$ ir siunčia T;
- T parenka $i = 0$ arba $i = 1$ ir siunčia I;
- Irena skaičiuoja $h \equiv j + ix \pmod{q}$ ir siunčia T;
- T tikrina

$$g^h \equiv y^i \gamma \pmod{n}.$$

Netiesioginis įrodymas

Bendra schema

Tikslas: Irena nori įrodyti T, kad žino sudėtingo uždavinio U sprendimą

- I panaudodama atsitiktinį skaičių r suformuluoja uždaviniui U ekvivalentų uždavinį $U(r)$ ir jį išsprendžia;
- I siunčia T uždavinį $U(r)$;
- T parenka bito b reikšmę ir siunčia I;
- Jei $b=0$, I siunčia T įrodymą, kad uždaviniai U ir $U(r)$ yra ekvivalentūs; jei $b = 1$, I siunčia $U(r)$ sprendimą;
- T tikrina, ar I įvykdė reikalavimą

Protokolas vykdomas n kartų.

Netiesioginis įrodymas

Visus protokolo žingsnius galima vykdyti iškart:

Tikslas: Irena nori įrodyti T, kad žino sudėtingo uždavinio U sprendimą

- I panaudodama atsitiktinius skaičius r_1, \dots, r_n suformuluoja uždaviniui U ekvivalentus uždavinius $U(r_i)$ ir juos išsprendžia;
- I siunčia T uždavinius $U(r_i)$;
- T parenka bitų b_1, \dots, b_n reikšmes ir siunčia I;
- Jei $b_i = 0$, I siunčia T įrodymą, kad uždaviniai U ir $U(r_i)$ yra ekvivalentūs; jei $b_i = 1$, I siunčia $U(r_i)$ sprendimą;
- T tikrina, ar I įvykdė reikalavimą.

Netiesioginis įrodymas be interaktyvumo

Tikslas: Irena nori įrodyti T, kad žino sudėtingo uždavinio U sprendimą.

Viešas įrankis: maišos funkcija h , kurianti n ilgio bitų santraukas.

- I panaudodama atsitiktinius skaičius r_1, \dots, r_n suformuluoja uždaviniui U ekvivalentinius uždavinius $U(r_i)$, juos išsprendžia;
- I skaičiuoja $h(U(r_1), \dots, U(r_n)) = (b_1, \dots, b_n)$;
- I paskelbia uždavinius $U(r_i)$;
- Jei $b_i = 0$, I paskelbia įrodymą, kad uždaviniai U ir $U(r_i)$ yra ekvivalentūs; jei $b_i = 1$, I paskelbia $U(r_i)$ sprendimą;

T gali nedalyvaujant I patikrinti, ar I paskelbė teisingus duomenis.

Netiesioginis įrodymas be interaktyvumo

Viešos žinios: p – pirminis skaičius, g – generuojantis elementas moduliui p , h -funkcija $h(u, v, w)$, įgyjanti reikšmes aibėje \mathbb{Z}_{p-1} ir y .

Irenos žinios: $x, g^x \equiv y \pmod{p}$.

Irena nori paskelbti netiesioginį įrodymą, kurį būtų galima patikrinti be interaktyvumo.

Irenos skaičiavimai:

- atsitiktinai parenka v , skaičiuoja $t \equiv g^v \pmod{p}$;
- skaičiuoja $c = h(g, y, t)$;
- skaičiuoja $r \equiv v - cx \pmod{p-1}$.

Irenos įrodymas, kad ji žino x yra (c, r) .

Netiesioginis įrodymas be interaktyvumo

Įrodymo tikrinimas:

- $t' \equiv g^r y^c \pmod{p}$;
- ar $c = h(g, y, t')$?

Netiesioginis įrodymas be interaktyvumo

p – pirminis skaičius, g – generuojantis elementas moduliui p ,
 h -funkcija $h(u_1, v_1, w_1, u_2, v_2, w_2)$, įgyjanti reikšmes aibėje \mathbb{Z}_{p-1}
ir y_1, y_2 ;

Irenos žinios: bent vienas iš elementų x_1, x_2 , $g^{x_i} \equiv y_i \pmod{p}$.
Irenos skaičiavimai įrodymui, kad ji žino bent vieną elementą x_i :

- atsitiktinai parenka v_1, v_2, w ;
- skaičiuoja: $t_1 \equiv y_1^w g^{v_1} \pmod{p}$, $t_2 \equiv g^{v_2} \pmod{p}$;
- $c = h(g_1, y_1, t_1, g_2, y_2, t_2)$;
- $c_1 = w, c_2 \equiv c - c_1 \pmod{p-1}$;
- $r_1 \equiv v_1 \pmod{p-1}, r_2 \equiv v_2 - c_2 x_2 \pmod{p-1}$.

Irenos įrodymas: (c_1, r_1, c_2, r_2) .

Netiesioginis įrodymas be interaktyvumo

Įrodymo tikrinimas:

- $t'_1 \equiv g^{r_1} y^{c_1} \pmod{p}$, $t'_2 \equiv g^{r_2} y^{c_2} \pmod{p}$;
- $c_1 + c_2 \equiv h(g_1, y_1, t'_1, g_2, y_2, t'_2) \pmod{p-1}$?

Netiesioginiai įrodymai (ZKP zero-knowledge proofs)

Reikalavimai skaitmeniniams pinigams

- autentiškumas: niekas negali pasiimti skaitmeninių pinigų mūsų vardu;
- vientisumas: sukurta pinigų negali būti pakeistas (prie 1 negali būti „prirašyta“ keletas nulių);
- tiesioginis mokėjimas: atsiskaitant skaitmeniniais pinigais, nereikia kreiptis į banką;
- saugumas: tie patys skaitmeniniai pinigai negali būti išleisti pakartotinai;
- anonimiškumas: atsiskaitant skaitmeniniais pinigais, neturi būti reikalinga informacija apie mokėtojus.

ECash skaitmeninių pinigų sistema

ECash sukūrė kompanija DigiCash.

A nori gauti skaitmeninių pinigų ir jais atsiskaityti už prekes ar paslaugas.

A turi uždirbti tikrų pinigų ir atsidaryti sąskaitą banke B, kad galėtų šiuos tikruosius pinigus versti skaitmeniniais.

Kad A vardu į banką, prašydamas skaitmeninių pinigų, negalėtų kreiptis Z, A turi naudotis kokia nors nustatyta autentifikavimo schema, pavyzdžiui, skaitmeniniais parašais.

Skaitmeninis parašas būtinas ir bankui B, kad būtų galima patvirtinti išduotų skaitmeninių banknotų tikrumą.

Tarkime, kad naudojama RSA skaitmeninių parašų schema.

ECash schemos skaitmeninių banknotų išdavimo protokolas

Tarkime, A nori gauti 100 EU skaitmeninį banknotą.

- A parengia n (banko nustatytą kiekį, pavyzdžiui, $n = 100$) skaitmeninių eilučių rinkinių $S_j = (I_{j1}, I_{j2}, \dots, I_{jn})$, $j = 1, \dots, n$; kiekvienoje eilutėje I_{jk} užrašyta A identifikuojanči informacija.
- Kiekviena eilutė I_{jk} kaip paslaptis padalijama į dvi dalis (L_{jk}, R_{jk}) .
- A parengia n banknotų po 100 EU: $M_j = (m_j, (L_{jk}, R_{jk})_{k=1, \dots, n})$, čia m_j yra skirtingi banknotų identifikavimo numeriai, juose sutartu būdu nurodyta ir banknoto vertė.
- A maskuoja banknotų numerius ir siunčia bankui $M_j^* = (z_j^e m_j, (L_{jk}, R_{jk})_{k=1, \dots, n})$, čia e yra banko B skaitmeninio parašo schemos viešasis raktas, z_j – A pasirinktas skaičius.

ECash schemos skaitmeninių banknotų išdavimo protokolas

- B atrenka $n - 1$ atsiųstą banknotą (pvz., M_1^*, \dots, M_{99}^*) ir pareikalauja, kad A nurodytų šiems banknotams kurti panaudotus maskuojančius daugiklius z_j .
- B patikrina, ar atrinktieji banknotai sudaryti teisingai: ar visuose juose nurodytos vienodos vertės ir visi numeriai skirtingi.
- Jeigu atskleistieji kvitai sudaryti teisingai, B pasirašo likusį ir siunčia A $((z_{100}^e m_{100})^d, (L_{100,k}, R_{100,k})_{k=1, \dots, n})$.
- A pašalina maskuojamąjį daugiklį ir turi skaitmeninį banknotą $(m_{100}, (m_{100})^d)$ ir dar tam tikrą jo „priedą“ $I_{100} = (L_{100,k}, R_{100,k})_{k=1, \dots, n}$.

ECash mokėjimo protokolas

- A pateikia pardavėjui P banknotą $(m_{100}, (m_{100})^d)$.
- P tikrina banko B parašą $m_{100} = ((m_{100})^d)^e$.
- P generuoja atsitiktinių bitų seką $b_1 b_2 \dots b_{100}$ ir perduoda A. Jeigu $b_i = 0$, A turi atskleisti $L_{100,i}$; jei $b_i = 1$, A turi atskleisti $R_{100,i}$.
- P siunčia B $(m_{100}, (m_{100})^d)$ ir atskleistas $I_{100,i}$ dalis.
- B taip pat patikrina parašą ir peržiūri savo duomenų bazę, ar pinigą su numeriu m_{100} dar nebuvo išleistas. Jeigu ne – perveda į P sąskaitą atitinkamą sumą, o į savo duomenų bazę įrašo atsiųstą informaciją. Jeigu jau išleistas – aiškinasi, kas kaltas.

Apgavystės atskleidimas

Jeigu B nustato, kad banknotas su tuo numeriu jau išleistas, jis lygina atsiųstas paslapties dalis su įrašytomis duomenų bazėje.

Jeigu visos jos sutampa – pardavėjas P bando banknotą išgryninti pakartotinai.

O jeigu nesutampa, tai banknotą bando pakartotinai panaudoti A. Tada iš pirmų nesutampančių paslapties dalių, tarkime, $L_{100,k}$ ir $R_{100,k}$, bankas nustato nesąžiningo kliento tapatybę.

Monetos metimo telefonu protokolas

Lošėjai A ir B.

Lošėjas A ir B parenka didelį pirminį skaičių ir du generuojančius elementus h ir s .

A atsitiktinai parenka skaičių x , skaičiuoja $y \equiv h^x \pmod{p}$ (arba $y \equiv s^x \pmod{p}$) ir siunčia B.

B spėja ar skaičiavimui buvo panaudotas h (herbas), ar s (skaičius).

A pasako ar įspėjo.

Kad B galėtų patikrinti, A atsiunčia x .

Elektroninis balsavimas

Reikalavimai elektroniniam balsavimui

- Balsuoti gali tik užsiregistravę rinkėjai
- Balsuoti galima tik kartą
- Niekas negali sužinoti, už ką balsavo rinkėjas
- Kiekvieno rinkėjo balsas turi būti užskaitytas
- Rinkėjas negali kopijuoti kito rinkėjo biuletenio
- Kiekvienas bandymas pakeisti biuletenius turi būti pastebėtas

I protokolas

Balsus skaičiuoja ir ataskaitas skelbia CRK - centrinė rinkiminė komisija.

- Rinkėjas šifruoja savo biuletenį naudodamas CRK viešąjį raktą
- CRK dešifruoja biuletenius, skaičiuoja balsus ir skelbia rezultatus.

II protokolas

- Rinkėjas pasirašo savo biuletenį privačiuoju raktu (pvz. RSA)
- Rinkėjas šifruoja biuletenį CRK viešuoju raktu ir siunčia CRK.
- CRK dešifruoja biuletenius, tikrina parašus, skaičiuoja balsus, skelbia rezultatus.

III protokolas

- Kiekvienas rinkėjas parengia n biuletenių. Kiekviename iš jų užrašomi visi galimi balsavimo rezultatai ir pakankamai ilgas atsitiktinis skaičius.
- Kiekvienas biuletenis yra maskuojamas ir siunčiamas CRK.
- CRK pareikalauja, kad rinkėjas atskleistų $n - 1$ -ą biuletenį. CRK tikrina, ar visi biuleteniai tinkamai sudaryti. Jeigu jie sudaryti teisingai - CRK pasirašo visus neatskleisto biuletenio elementus ir siunčia rinkėjui atgal.
- Rinkėjas pašalina paskutiniojo biuletenio maskuotę, pasirenka jo nuomonę atitinkantį sprendimą, jį šifruoja (taip pat ir biuletenio atsitiktinį skaičių) CRK viešuoju raktu ir siunčia CRK.
- CRK dešifruoja biuletenį, tikrina parašą, tikrina, ar biuletenio skaičiaus dar nėra duomenų bazėje, skaičiuoja ir skelbia rezultatus. Kartu nurodomi biuletenių skaičiai, kad rinkėjas galėtų patikrinti, ar jo balsas įskaitytas tinkamai.

IV protokolas

- CRK paskelbia rinkėjų registravimosi pradžia
- Iki nurodytos datos rinkėjai registruojasi
- Kiekvienas rinkėjas iš CRK gauna pvz. dvidešimties skaitmenų ilgio identifikacijos numerį I (naudojant aklo parašo protokolą)
- Kiekvienas rinkėjas generuoja RSA raktus n, e, d .
- Rinkėjas balsuoja, siųsdamas CRK I ir $e(I, v|e)$, čia v yra kandidatas, už kurį balsuojama
- CRK praneša apie gautus balsus publikuodama $I, e(I, v|e)$.
- Rinkėjas siunčia CRK I, d .
- CRK dešifruoja balsus ir kiekvienam v publikuoja sąrašą $I, e(I, v|e)$
- Rinkėjai patikrina, ar jų balsai teisingai įskaityti

Lošimo kortomis „telefonu“ protokolas

Protokolą sudaro trys dalys:

- Kortų dalijimas
- Kortų atskleidimas
- Lošimo korektiškumo tikrinimas

Kortų dalijimas

Reikia A ir B duoti po k atsitiktinai parinktų kortų.

- A ir B susitaria dėl bendro pirminio skaičiaus p ir kiekvienas pasirenka po porą Diffie-Hellmano kriptosistemos raktų $K_A = \langle e_A, d_A \rangle$, $K_B = \langle e_B, d_B \rangle$

$$e_A d_A \equiv 1 \pmod{(p-1)}, e_B d_B \equiv 1 \pmod{(p-1)}.$$

- A užšifruoja žinutes-kortų pavadinimus m_1, m_2, \dots, m_n , išrašytus atsitiktine tvarka ir siunčia B šifrus $c_i \equiv m_i^{e_A} \pmod{p}$.
- B atrenka k skaičių c_i ir nusiunčia A.
- A iššifruoja c_i ir žino, kokios kortos jam teko.

Kortų dalijimas

- Po to B atrenka dar k kortų ir jas užšifruoja:

$$c'_i \equiv c_i^{e_B} \pmod{p}$$

ir siunčia A.

- A iššifruoja gautas žinutes:

$$c_i^* \equiv (c_i)^{d_A} \pmod{p}$$

ir siunčia atgal B.

- B iššifruoja

$$m_i \equiv (c_i^*)^{d_B} \pmod{p}$$

ir žino, kokios kortos B teko.

Kortos atskleidimas ir korektiškumo tikrinimas

Kai A daro ėjimą (atskleidžia kortą) siunčia partneriui porą $\langle m_i, c_i \rangle$, $c_i \equiv m_i^{e_A} \pmod{p}$.

Analogiškai elgiasi ir B.

Kai lošimas baigiasi, partneriai turi pasikeisti raktais, kad galėtų patikrinti, ar buvo lošta tomis kortomis, kurias jie turėjo.