

ISSN 1991-346X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

**ФИЗИКА-МАТЕМАТИКА
СЕРИЯСЫ**



СЕРИЯ

ФИЗИКО-МАТЕМАТИЧЕСКАЯ



**PHYSICO-MATHEMATICAL
SERIES**

3 (307)

МАМЫР – МАУСЫМ 2016 ж.

МАЙ – ИЮНЬ 2016 г.

MAY – JUNE 2016

1963 ЖЫЛДЫҢ ҚАҢТАР АЙЫНАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С ЯНВАРЯ 1963 ГОДА
PUBLISHED SINCE JANUARY 1963

ЖЫЛЫНА 6 РЕТ ШЫҒАДЫ
ВЫХОДИТ 6 РАЗ В ГОД
PUBLISHED 6 TIMES A YEAR

АЛМАТЫ, ҚР ҰҒА
АЛМАТЫ, НАН РК
ALMATY, NAS RK

Б а с р е д а к т о р

ҚР ҰҒА академигі,

Мұтанов Г. М.

Р е д а к ц и я а л қ а с ы:

физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Әшімов А.А.**; техн. ғ. докторы, проф., ҚР ҰҒА академигі **Байғұнчечков Ж.Ж.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Жұмаділдаев А.С.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Қалменов Т.Ш.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Мұқашев Б.Н.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Өтелбаев М.О.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Тәкібаев Н.Ж.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Харин С.Н.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Әбішев М.Е.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Жантаев Ж.Ш.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Қалимолдаев М.Н.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Косов В.Н.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Мұсабаев Т.А.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Ойнаров Р.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Рамазанов Т.С.** (бас редактордың орынбасары); физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Темірбеков Н.М.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Өмірбаев У.У.**

Р е д а к ц и я к ең е с і:

Украинаның ҰҒА академигі **И.Н. Вишневский** (Украина); Украинаның ҰҒА академигі **А.М. Ковалев** (Украина); Беларусь Республикасының ҰҒА академигі **А.А. Михалевич** (Беларусь); Әзірбайжан ҰҒА академигі **А. Пашаев** (Әзірбайжан); Молдова Республикасының ҰҒА академигі **И. Тигиняну** (Молдова); мед. ғ. докторы, проф. **Иозеф Банас** (Польша)

Главный редактор

академик НАН РК

Г. М. Мутанов

Редакционная коллегия:

доктор физ.-мат. наук, проф., академик НАН РК **А.А. Ашимов**; доктор техн. наук, проф., академик НАН РК **Ж.Ж. Байгунчеков**; доктор физ.-мат. наук, проф., академик НАН РК **А.С. Джумадильдаев**; доктор физ.-мат. наук, проф., академик НАН РК **Т.Ш. Кальменов**; доктор физ.-мат. наук, проф., академик НАН РК **Б.Н. Мукашев**; доктор физ.-мат. наук, проф., академик НАН РК **М.О. Отелбаев**; доктор физ.-мат. наук, проф., академик НАН РК **Н.Ж. Такибаев**; доктор физ.-мат. наук, проф., академик НАН РК **С.Н. Харин**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **М.Е. Абишев**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **Ж.Ш. Жантаев**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **М.Н. Калимолдаев**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **В.Н. Косов**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **Т.А. Мусабаев**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **Р. Ойнаров**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **Т.С. Рамазанов** (заместитель главного редактора); доктор физ.-мат. наук, проф., чл.-корр. НАН РК **Н.М. Темирбеков**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **У.У. Умирбаев**

Редакционный совет:

академик НАН Украины **И.Н. Вишневский** (Украина); академик НАН Украины **А.М. Ковалев** (Украина); академик НАН Республики Беларусь **А.А. Михалевич** (Беларусь); академик НАН Азербайджанской Республики **А. Пашаев** (Азербайджан); академик НАН Республики Молдова **И. Тигиняну** (Молдова); д. мед. н., проф. **Иозеф Банас** (Польша)

«Известия НАН РК. Серия физико-математическая». ISSN 1991-346X

Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан №5543-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год.

Тираж: 300 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18,

www.nauka-nanrk.kz/physics-mathematics.kz

© Национальная академия наук Республики Казахстан, 2016

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

Editor in chief

G. M. Mutanov,
academician of NAS RK

Editorial board:

A.A. Ashimov, dr. phys-math. sc., prof., academician of NAS RK; **Zh.Zh. Baigunchekov**, dr. eng. sc., prof., academician of NAS RK; **A.S. Dzhumadildayev**, dr. phys-math. sc., prof., academician of NAS RK; **T.S. Kalmenov**, dr. phys-math. sc., prof., academician of NAS RK; **B.N. Mukhashev**, dr. phys-math. sc., prof., academician of NAS RK; **M.O. Otelbayev**, dr. phys-math. sc., prof., academician of NAS RK; **N.Zh. Takibayev**, dr. phys-math. sc., prof., academician of NAS RK; **S.N. Kharin**, dr. phys-math. sc., prof., academician of NAS RK; **M.Ye. Abishev**, dr. phys-math. sc., prof., corr. member of NAS RK; **Zh.Sh. Zhantayev**, dr. phys-math. sc., prof., corr. member of NAS RK; **M.N. Kalimoldayev**, dr. phys-math. sc., prof., corr. member of NAS RK; **V.N. Kosov**, dr. phys-math. sc., prof., corr. member of NAS RK; **T.A. Mussabayev**, dr. phys-math. sc., prof., corr. member of NAS RK; **R. Oinarov**, dr. phys-math. sc., prof., corr. member of NAS RK; **T.S. Ramazanov**, dr. phys-math. sc., prof., corr. member of NAS RK (deputy editor); **N.M. Temirbekov**, dr. phys-math. sc., prof., corr. member of NAS RK; **U.U. Umirbayev**, dr. phys-math. sc., prof., corr. member of NAS RK

Editorial staff:

I.N. Vishnievski, NAS Ukraine academician (Ukraine); **A.M. Kovalev**, NAS Ukraine academician (Ukraine); **A.A. Mikhalevich**, NAS Belarus academician (Belarus); **A. Pashayev**, NAS Azerbaijan academician (Azerbaijan); **I. Tighineanu**, NAS Moldova academician (Moldova); **Joseph Banas**, prof. (Poland).

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 1991-346X

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)

The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 5543-Ж, issued 01.06.2006

Periodicity: 6 times a year

Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
www.nauka-nanrk.kz / physics-mathematics.kz

© National Academy of Sciences of the Republic of Kazakhstan, 2016

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN

PHYSICO-MATHEMATICAL SERIES

ISSN 1991-346X

Volume 3, Number 307 (2016), 23 – 29

UDC 004.056.55

CRYPTANALYSIS OF ENCRYPTION SYSTEMS

A. M. Akhmetova, S.A. Nugmanova

Institute of information and computational technologies CS MES RK, Almaty
Kazakh national pedagogical university named after Abay, Almaty
ardak_66@mail.ru, nugm_s@mail.ru

Key words: informative safety, confidentiality of information, open key, secret key, cryptography with the symmetric keys.

Abstract. In the modern world informative safety becomes the major base element of all system of national safety of any state. It, foremost, is bound by growing like a weed technological possibilities of the modern informative systems. A review and analysis of existent methods of defense of information a cryptographic method are in-process examined.

An encipherment with the use of the key can help to keep secrets out of harm's way, but if it is needed together to use secret information with other people, it is necessary also together to use the keys. But how safely to send to the keys other people? Some decisions are described in this article, including conception of cryptography with the key.

To decide the task of distribution of the keys, it is possible to use cryptography with the key, In algorithm data, in cipher by means of the key, can be deciphered only by means of the secret key. Only interactive parties can create this secret value that after will be used.

ӘОЖ 004.056.55

ШИФРЛАУ ЖҮЙЕСІНЕ КРИПАНАЛИЗ ЖАСАУ

А.М. Ахметова, С.А. Нугманова

ҚР ҒК БЖҒМ Ақпараттық және есептеу технологиясы институты, Алматы
Абай атындағы ҚазҰПУ, Алматы

Түйін сөздер: ақпараттық қауіпсіздік, ақпараттың конфиденциалдылығы, ашық кілт, құпия кілт, симметриялы кілт бар криптография, криптоанализ, инициализациялау, интерпретация.

Аннотация. Кілтті пайдалану арқылы шифрлау мәліметтердің қауіпсіздігін сақтауға септігін тигізеді және ол басқа қолданушыға құпия ақпаратты білуге жол бермейді, сондай-ақ онымен қоса кілттерді пайдалануға болады. Бірақ басқа қолданушыға қалайша кілтті қауіпсіз жіберуге болады? Бұл мақалада кілттер криптографиясы қарастырылады.

Кілттерді үлестіру есебін шығару үшін кілттер криптографиясын қарастыруға болады. Кілтпен шифрлау деректер алгоритмі тек құпия кілтін пайдаланып қабылдамау мүмкін. Тек өзара байланыс жасаушы тараптар бұл құпияның мәнін жасай алады, содан кейін сессия кілт ретінде пайдаланылуы мүмкін.

Әрбір криптоанализде алгоритмнің артықшылықтары мен кемшіліктері бар, сондықтан бұл алгоритмдердің бір-бірінен артықшылығы белгілі бір қолдану үшін таңдалады. Егер құпиясөздің кілттерін сақтайтын жоғалған құрылғыны ұмытылса криптографиялық кілттердің жоғалту мүмкіндігі бар. Сонымен қатар, ақпараттық шифрланған кілттерді қалпына келтіру керек болуы мүмкін. Осы себептерге байланысты, көптеген ұйымдар қайта қалпына келтіру кілттерінің жоспарларын іске асыруда. Әдетте, қысқарту негізгі пайдалануды көздейді, кілт қалпына келтіру агентті пайдаланып кілттерді шифрлайды.

Кіріспе. Криптоанализ кілтімен байланысты, сызықты криптоанализ, шабуылға тұрақты қасиеті бар дифференциалды криптоанализ ретінде ұсынылады, криптожүйелер (SPN) желісінде DES-орнын ауыстыруды, CAST-128 алгоритмі шифрлау ретінде құжат болады. Бұл шифр сондай-ақ, басқа да бірқатар керекті қасиеттерге ие, криптографиялық, оның ішінде, қатаң сынға (SAC), Бит (БИК) сыныға тәуелсіз комплементация емес меншік, кілтердің әлсіз және жартылай әлсіз болмауы Адамс [Адамс] кейбір егжей-тегжейлі Cast есептеу әдіснамасын талқылайды.

Зерттеу әдісі.

Алгоритмнің сипаттамасы.

CAST-128 агоритмі танымал Фейстел шифрі шифрлау алгоритмдерінің классына жатады. Жалпы жұмыс шифрлау стандартына (DES) ұқсас. Стандартты шифрда көрсетілгендей толық шифрлау алгоритмі төмендегідей төрт қадамда келтірілген.

Енгізілген: ашық мәтін $M_1 \dots M_{64}$; = K_1 кілті $K \dots K_{128}$

Шығыста: шифрленген мәтінді $C_1 \dots C_{64}$.

1. (график кілті) K ден { K_{13} , $K_{ри}$ } 16 жұп бөлімшесі есептеледі.

2. $(L_0, r_0) \leftarrow (M_1 \dots M_{64})$ (Сплит ашық мәтінін) солға, ($L_0 = M_1 \dots M_{32}$ и $M_{33} R_0 = \dots m_{64}$).

32- разрядтың жартысы оңға

3. (16 тур) 1-ден 16-ға дейінгі i үшін L_i және R_i мынадай түрде келесі есептеледі $L_i = R_{i-1}$;

$R_i = L_{i-1} \wedge F(R_{i-1}, K_{mi}, Кри)$, F -те анықталады. (F - 1тип, 2 типті немесе 3тип i -ге байланысты).

4. $C_1 \dots C_{64} \leftarrow (R_{16}, L_{16})$. (Қорытынды блоктар курсы L_{16} , R_{16} және шифрленген мәтінді

калыптастыру, біріктіру). Жоғарыда кетірілген шифрланған алгоритм шифрды ашу алгоритмімен бірдей, сонымен қатар ол (бөлімшелердің жұбы демек тізбектелген), (R_{16}, L_{16}) және (C_0, R_0) есептеу үшін кері тәртіппен пайдаланылады. Жасау үшін пайдаланылуы мүмкін тест векторлар B қосымшасында қараңыз. Осы алгоритмнің іске асыру дұрыстығы.

Жұп кілттер раунды.

CAST-128 де бөлімшелердің жұбы раундта қолданылады: маска ретінде $K.M$ пайдаланылады.

32 биттік сан болып табылады. «Кілтті «айналу» Kp пайдаланылады 5биттік кілт сан.

Бірдей раундтар номері.

CAST-128 де тек үш түрлі функцияларды пайдаланылады. Раундтың келесідей (кіші байт арқылы « Id », ең маңызды байт "ИА" f и функциясы, деректердің кіріс "D" тиесілі). Назар аударыңыз, яғни «+» және «-» қосу және азайту 2 модулі бойынша ** 32, «^» А Биттік НЕМЕСЕ және «<<<<» дөңгелек сол жақ болып табылады.

Жұмыс жалғасады.

Тип 1: $Y = ((K_{mi} + D) \lll Кри)$

$F = ((S_1 [IA] \wedge S_2 [Ib]) - S_3 [Ic]) + S_4 [ID]$

Тип 2: $Y = ((K_{mi} \wedge D) \lll Кри)$

$F = ((S_1 [IA] - S_2 [Ib]) + S_3 [Ic]) \wedge S_4 [ID]$

Тип 3: $Y = ((K_{mi} - D) \lll Кри)$

$F = ((S_1 [IA] + S_2 [Ib]) \wedge S_3 [Ic]) - S_4 [ID]$

Туры 1, 4, 7, 10, 13, и 16 қолданылатын функция F Тип 1.

Туры 2, 5, 8, 11, и 14 қолданылатын функция F Тип 2.

Туры 3, 6, 9, 12, и 15 қолданылатын функция F Тип 3.

Ауыстыру қорабы

CAST-128 сегіз алмастыру қорапбы пайдаланады: : S -қорабының график кілті болып табылады, S_5, S_6, S_7, S_8 S -боксы функциясы дөңгелектелген S -б Тек 4 Кбайт нақты шифрлеу кезінде қажетті екенін ескеріңіз оқы; және S_1, S_2, S_3, S_4 және S -қорапбы. Дегенмен 8 S -қораптар 8 килобайт жады жалпы талап етеді. Тек 4 Кбайт нақты шифрлеу кезінде қажетті екенін ескеріңіз, деректерді енгізуден бұрын шифрды ашу бірнеше қосалқы бөліктен бөлініп жасалады. $S_1 - S_8, S$ -блоктар. мазмұнына A қосымшасынан қараңыз.

Кілт кестесі

128-биттік кілт былай болса $x_0x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{Ax}x_{Bx}x_{Cx}x_{Dx}x_{Ex}x_{F}$, онда x_0 ең үлкен байт XF ең маңызды байт болып табылады.

Былай болса, $Z_0..z_F$ аралық болсын (уақытша) байт.

$S_i []$ ұсынады S -Box, онда «^» болса, XOR қосуды білдіреді.

Кілт мына түінінен құралса $x_0x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{Ax}x_{Bx}x_{Cx}x_{Dx}x_{Ex}x_{F}$ келесідей болады.

$$\begin{aligned}
z0z1z2z3 &= x0x1x2x3 \wedge S5 [XD] \wedge S6 [XF] \wedge S7 [xc] \wedge S8 [xE] \wedge S7 [x8] \\
z4z5z6z7 &= x8x9xAxB \wedge S5 [z0] \wedge S6 [Z2] \wedge S7 [Z1] \wedge S8 [Z3] \wedge S8 [xД] \\
z8z9zAzB &= xCxDxExF \wedge S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S5 [x9] \\
zCzDzEzF &= x4x5x6x7 \wedge S5 [ZA] \wedge S6 [z9] \wedge S7 [ZB] \wedge S8 [Z8] \wedge S6 [BP] \\
K1 &= S5 [Z8] \wedge S6 [z9] \wedge S7 [Z7] \wedge S8 [Z6] \wedge S5 [Z2] \\
K2 &= S5 [ZA] \wedge S6 [ZB] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S6 [Z6] \\
K3 &= S5 [ZC] \wedge S6 [ZD] \wedge S7 [Z3] \wedge S8 [Z2] \wedge S7 [z9] \\
K4 &= S5 [ZE] \wedge S6 [rP] \wedge S7 [Z1] \wedge S8 [z0] \wedge S8 [ZC] \\
x0x1x2x3 &= z8z9zAzB \wedge S5 [Z5] \wedge S6 [Z7] \wedge S7 [Z4] \wedge S8 [Z6] \wedge S7 [z0] \\
x4x5x6x7 &= z0z1z2z3 \wedge S5 [x0] \wedge S6 [x2] \wedge S7 [x1] \wedge S8 [x3] \wedge S8 [Z2] \\
x8x9xAxB &= z4z5z6z7 \wedge S5 [x7] \wedge S6 [x6] \wedge S7 [x5] \wedge S8 [x4] \wedge S5 [Z1] \\
xCxDxExF &= zCzDzEzF \wedge S5 [xД] \wedge S6 [x9] \wedge S7 [BP] \wedge S8 [x8] \wedge S6 [z3] \\
K5 &= S5 [x3] \wedge S6 [x2] \wedge S7 [xc] \wedge S8 [XD] \wedge S5 [x8] \\
K6 &= S5 [x1] \wedge S6 [x0] \wedge S7 [xE] \wedge S8 [XF] \wedge S6 [XD] \\
K7 &= S5 [x7] \wedge S6 [x6] \wedge S7 [x8] \wedge S8 [x9] \wedge S7 [x3] \\
K8 &= S5 [x5] \wedge S6 [x4] \wedge S7 [xД] \wedge S8 [BP] \wedge S8 [x7] \\
z0z1z2z3 &= x0x1x2x3 \wedge S5 [XD] \wedge S6 [XF] \wedge S7 [xc] \wedge S8 [xE] \wedge S7 [x8] \\
z4z5z6z7 &= x8x9xAxB \wedge S5 [z0] \wedge S6 [Z2] \wedge S7 [Z1] \wedge S8 [Z3] \wedge S8 [xД] \\
z8z9zAzB &= xCxDxExF \wedge S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S5 [x9] \\
zCzDzEzF &= x4x5x6x7 \wedge S5 [ZA] \wedge S6 [z9] \wedge S7 [ZB] \wedge S8 [Z8] \wedge S6 [BP] \\
K9 &= S5 [Z3] \wedge S6 [Z2] \wedge S7 [ZC] \wedge S8 [ZD] \wedge S5 [z9] \\
K10 &= S5 [Z1] \wedge S6 [z0] \wedge S7 [ZE] \wedge S8 [rP] \wedge S6 [ZC] \\
K11 &= S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z8] \wedge S8 [z9] \wedge S7 [Z2] \\
K12 &= S5 [Z5] \wedge S6 [Z4] \wedge S7 [ZA] \wedge S8 [ZB] \wedge S8 [Z6] \\
x0x1x2x3 &= z8z9zAzB \wedge S5 [Z5] \wedge S6 [Z7] \wedge S7 [Z4] \wedge S8 [Z6] \wedge S7 [z0] \\
x4x5x6x7 &= z0z1z2z3 \wedge S5 [x0] \wedge S6 [x2] \wedge S7 [x1] \wedge S8 [x3] \wedge S8 [Z2] \\
x8x9xAxB &= z4z5z6z7 \wedge S5 [x7] \wedge S6 [x6] \wedge S7 [x5] \wedge S8 [x4] \wedge S5 [Z1] \\
xCxDxExF &= zCzDzEzF \wedge S5 [xД] \wedge S6 [x9] \wedge S7 [BP] \wedge S8 [x8] \wedge S6 [z3] \\
K13 &= S5 [x8] \wedge S6 [x9] \wedge S7 [x7] \wedge S8 [x6] \wedge S5 [x3] \\
K14 &= S5 [xД] \wedge S6 [BP] \wedge S7 [x5] \wedge S8 [x4] \wedge S6 [x7] \\
K15 &= S5 [xc] \wedge S6 [XD] \wedge S7 [x3] \wedge S8 [x2] \wedge S7 [x8] \\
K16 &= S5 [xE] \wedge S6 [XF] \wedge S7 [x1] \wedge S8 [x0] \wedge S8 [XD]
\end{aligned}$$

[Қалған жартысы жоғарыда көрсетілгенмен бірдей, K17 - K32 кілттерді құру үшін соңғы құрылғанмен бірдей x0...xF].

$$\begin{aligned}
z0z1z2z3 &= x0x1x2x3 \wedge S5 [XD] \wedge S6 [XF] \wedge S7 [xc] \wedge S8 [xE] \wedge S7 [x8] \\
z4z5z6z7 &= x8x9xAxB \wedge S5 [z0] \wedge S6 [Z2] \wedge S7 [Z1] \wedge S8 [Z3] \wedge S8 [xД] \\
z8z9zAzB &= xCxDxExF \wedge S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S5 [x9] \\
zCzDzEzF &= x4x5x6x7 \wedge S5 [ZA] \wedge S6 [z9] \wedge S7 [ZB] \wedge S8 [Z8] \wedge S6 [BP] \\
K17 &= S5 [Z8] \wedge S6 [z9] \wedge S7 [Z7] \wedge S8 [Z6] \wedge S5 [Z2] \\
K18 &= S5 [ZA] \wedge S6 [ZB] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S6 [Z6] \\
K19 &= S5 [ZC] \wedge S6 [ZD] \wedge S7 [Z3] \wedge S8 [Z2] \wedge S7 [z9] \\
K20 &= S5 [ZE] \wedge S6 [rP] \wedge S7 [Z1] \wedge S8 [z0] \wedge S8 [ZC] \\
x0x1x2x3 &= z8z9zAzB \wedge S5 [Z5] \wedge S6 [Z7] \wedge S7 [Z4] \wedge S8 [Z6] \wedge S7 [z0] \\
x4x5x6x7 &= z0z1z2z3 \wedge S5 [x0] \wedge S6 [x2] \wedge S7 [x1] \wedge S8 [x3] \wedge S8 [Z2] \\
x8x9xAxB &= z4z5z6z7 \wedge S5 [x7] \wedge S6 [x6] \wedge S7 [x5] \wedge S8 [x4] \wedge S5 [Z1] \\
xCxDxExF &= zCzDzEzF \wedge S5 [xД] \wedge S6 [x9] \wedge S7 [BP] \wedge S8 [x8] \wedge S6 [z3] \\
K21 &= S5 [x3] \wedge S6 [x2] \wedge S7 [xc] \wedge S8 [XD] \wedge S5 [x8] \\
K22 &= S5 [x1] \wedge S6 [x0] \wedge S7 [xE] \wedge S8 [XF] \wedge S6 [XD] \\
K23 &= S5 [x7] \wedge S6 [x6] \wedge S7 [x8] \wedge S8 [x9] \wedge S7 [x3] \\
K24 &= S5 [x5] \wedge S6 [x4] \wedge S7 [xД] \wedge S8 [BP] \wedge S8 [x7] \\
z0z1z2z3 &= x0x1x2x3 \wedge S5 [XD] \wedge S6 [XF] \wedge S7 [xc] \wedge S8 [xE] \wedge S7 [x8] \\
z4z5z6z7 &= x8x9xAxB \wedge S5 [z0] \wedge S6 [Z2] \wedge S7 [Z1] \wedge S8 [Z3] \wedge S8 [xД] \\
z8z9zAzB &= xCxDxExF \wedge S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z5] \wedge S8 [Z4] \wedge S5 [x9]
\end{aligned}$$

$$\begin{aligned} zCzDzEzF &= x_4x_5x_6x_7 \wedge S5 [ZA] \wedge S6 [z_9] \wedge S7 [ZB] \wedge S8 [Z8] \wedge S6 [BP] \\ K25 &= S5 [Z3] \wedge S6 [Z2] \wedge S7 [ZC] \wedge S8 [ZD] \wedge S5 [z_9] \\ K26 &= S5 [Z1] \wedge S6 [z_0] \wedge S7 [ZE] \wedge S8 [rP] \wedge S6 [ZC] \\ K27 &= S5 [Z7] \wedge S6 [Z6] \wedge S7 [Z8] \wedge S8 [z_9] \wedge S7 [Z2] \\ K28 &= S5 [Z5] \wedge S6 [Z4] \wedge S7 [ZA] \wedge S8 [ZB] \wedge S8 [Z6] \\ x_0x_1x_2x_3 &= z_8z_9zAzB \wedge S5 [Z5] \wedge S6 [Z7] \wedge S7 [Z4] \wedge S8 [Z6] \wedge S7 [z_0] \\ x_4x_5x_6x_7 &= z_0z_1z_2z_3 \wedge S5 [x_0] \wedge S6 [x_2] \wedge S7 [x_1] \wedge S8 [x_3] \wedge S8 [Z2] \\ x_8x_9xAxB &= z_4z_5z_6z_7 \wedge S5 [x_7] \wedge S6 [x_6] \wedge S7 [x_5] \wedge S8 [x_4] \wedge S5 [Z1] \\ xCxDxExF &= zCzDzEzF \wedge S5 [xD] \wedge S6 [x_9] \wedge S7 [BP] \wedge S8 [x_8] \wedge S6 [z_3] \\ K29 &= S5 [x_8] \wedge S6 [x_9] \wedge S7 [x_7] \wedge S8 [x_6] \wedge S5 [x_3] \\ K30 &= S5 [xD] \wedge S6 [BP] \wedge S7 [x_5] \wedge S8 [x_4] \wedge S6 [x_7] \\ K31 &= S5 [xc] \wedge S6 [XD] \wedge S7 [x_3] \wedge S8 [x_2] \wedge S7 [x_8] \\ K32 &= S5 [xE] \wedge S6 [XF] \wedge S7 [x_1] \wedge S8 [x_0] \wedge S8 [XD] \end{aligned}$$

Зерттеу нәтижесі.

Жасырынған бөлімдер және бұрмаланған бөлімдер.

Km1, ..., Km16 болса 32-разрядты жасырылған бөлімшелер (раундқа біреу).

Km1, ..., Km16 болса 32 -бит бөлімшелер бұрмалау (раундқа біреу).

Тек кіші 5 бит пайдаланылады әрбір раундт үшін (я = 1; я <= 16; я ++) {Kmi = Ki; Kpi = K16 + я; }

Айнымалы KeySize

кілтті мүмкіндік беру үшін жасалған CAST-128 шифрлау алгоритмі болатын.

8-бит қадаммен 40тан 128 битке өзгеріліп отыруы мүмкін мөлшері, (Яғни, рұқсат етілген негізгі кілт өлшемі 40, 48, 56, 64, ..., 112, 120, және 128 бит. болып табылады.

Айнымалы жұмыс үшін KeySize ерекшелігі келесідей

1) негізгі өлшемдері үшін, 80 бит (яғни, 40, 48, 56, 64-ге дейін

72 және 80 бит), нақты алгоритм сипатталған, бірақ пайдалана

12; раундтың орнына 16қолданылады;

2) 80 бит-ден артық негізгі өлшемдері үшін, содан кейін алгоритм толық 16 пайдаланады;

3) 128 бит-тен кем негізгі өлшемдеріне, кілті нөл байт толтырады отыр

(оң немесе, кем дегенде, маңызды, ережелер) үшін

128 бит (кіріс кілтті 128 бит ұсынады ал CAST-128 кілт графгі)

Дегенмен CAST-128 барлық тізімдегі 12 өлшеміндегі кілті қолдайтыны мүмкін екенін ескеріңіз.

Жоғарыда, 40 бит, 64 бит, 80 бит және 128 бит, өлшемдері типтік шартты қолдануды табу.

Осылайша ең алдымен бұл төрт өлшемдерді жиынында қолдау үшін көпшілікті жүзеге асыру жеткілікті болады.

Операцияда айнымалы өлшемінің негізгін пайдаланған кезде шатастырмас үшін, CAST-128 атауын CAST5 атауы синонимі ретінде қарастырылуы тиіс;

екі мағыналы емес, қасылатын кілт өлшемін береді. Осылайша мысалы CAST-128 40-бит кілтімен CAST5-40 деп аталады;

128-биттік кілт анық арналған, онда аты CAST5-128 пайдаланылған тиіс.

CAST5 нысана идентификаторы.

Кімде кім CAST алгоритмін прокол ретінде хабарласуға қолданса немесе басқа контексте пайдаланса онда нысана идентификаторы кесі түрде OID анықталған.

Нысана идентификатор алгоритмі ::=

{ISO (1) memberBody (2) США (840) NT (113533) NSN (7) алгоритмі (66)}

cast5CBC нысана идентификатор ::= {алгоритм cast5CBC (10)}

Параметрі:: = тізбектелінуі {IV ОКТЕТ жол келісім бойынша 0, инициализация- векторы

Кілт ұзындығы бүтін сан – кілт ұзындығы }

Ескерту: IV міндеті емес және келісім бойынша барлығы үшін нөл.

Болмауға тиіс, IV егер барлық нөлдерді пайдаланғанда кодтау соңында.

Параметрлер. Декодтау соңында Iv болмауы керек, интерпретацияланады барлық нөлдер ретінде түсіндіріледі.

CBC режимінде бұл шифрлеу және дешифрлеу симметриялық алгоритм блок шифры.

CAST-128 пайдаланып. cast5MAC идентификатор нысаны:: = {алгоритмдері cast5MAC (11)}

Параметрі:: = тізбектелген {macLength сан, - ұзындықПДК, битте

Кілттің ұзындығы бүтін сан- бит негізгі ұзындығы}

Симметриялық блок Cast-128 шифрлау алгоритмі пайдаланылған хабар аутентификациясы.

pbeWithMD5AndCast5CBC идентификатор нысаны :: =

Параметрі:: = тізбектелген {Октетов жол

iterationCount сан, хэш - итерацияларының жалпы саны –

Кілттің ұзындығы бүтін сан- бит негізгі ұзындығы}

Ескерту: IV хештау процедурасынан алынған, сондықтан да параметрлерін енгізілуі қажет емес.

Ол CBC режимінде құпия пароль сөз шифрлау мен шифрді шешу негізделген MD5 және CAST128 симметриялық блокты шифр пайдалану.

Толығырақ PBE есептеу үшін (DES алгоритмі пайдаланады) PKCS5 қараңыз.

Тест векторлары. Бұл бағдарлама сипатталған CAST-128 шифр үшін тест векторы қамтамасыз ететін құжат.

Холост жинақтары Plaintext-Key -шифрланған мәтін

Алгоритм дұрыс орындалып жатқанын, қамтамасыз ету үшін, Мынадай төмендегі тесті векторлары берілген, тексеру үшін пайдалануға болады (Оналтылық санау жүйесінде көрсетілген).

128-биттік кілт = 23 45 01 67 12 34 56 78 23 45 67 89 34 56 78 9A

Ашық мәтін = 01 23 45 67 89 AB CD EF

шифрланған мәтін (жабық мәтін). = 23 8B 4F E5 84 7E 44 B2

80-биттік кілт = 23 45 01 67 12 34 56 78 23 45

= 01 23 45 67 12 34 56 78 23 45 00 00 00 00 00 00

Ашық мәтін = 01 23 45 67 89 AB CD EF

шифрланған мәтін (жабық мәтін). = 7A C8 16 D1 6E 9B 30 2E

БИ 2 сынаққа толық қызмет көрсету

Тексеруде тестте CAST-128 техникалық қызмет көрсету анықталды.

Іске асыру дұрыстығы. Ол псевдо-код анықталады,

Онда a және b 128-биттік векторлар болып табылады тиіс, A1 және AP сол және оң жартысы болады, BL және BR сол және оң жартысы b және шифр (D, K) болады шифрлау режимінде ECB

Блокта D кілтті асты K. шифрлау болып табылады.

Бастапқы a = 01 23 45 67 12 34 56 78 23 45 67 89 34 56 78 9A (HEX)

Бастапқы b = 01 23 45 67 12 34 56 78 23 45 67 89 34 56 78 9A (HEX)

1000000 рет істеу

{ aB = шифрлеу (A1, b)

AR = шифрлеу (Ar, b)

BL = шифрлеу (BL, a)

Марка = шифрлеу (Марка, a)}

Көз жеткізідік, v == E. A9 D0 A2 3B 49 FO A6 B3 43 6F B8 9D 6D Калифорния 92 (он алтылық)

Көз жеткізідік, b == B2 C9 5E B0 0C 31 AD 71 80 05 AC B8 E8 3D 69 6E (HEX)

== E. A9 A2 D0 3B 49 43 FD A6 B3 B8 9D 6D 6F Калифорния 92 (он алтылық)

Талқылау. CAST-128 блок өлшемін бар 12- немесе 16-раундты Фейстел желісі болып табылады, Блок негізгі мөлшері 64 бит, кілт өлшемі 128 бит; қамтамасыз ету үшін айналуын пайдаланады. Сызықтық және дифференциалдық ішінен шабуылдарға тұрақты пайдаланады. Қоспасы функциясы (**) 32 бойынша 2 модулі XOR, қосу және азайтуды қолданылады; және шифрлау кезеңінде функцияның үш фазалы өзгермелілігі түрленуі пайдаланады. Соңында, 8x32 S-боксы раунды қолданылады. 2 кестесінде таратудың айырмашылығы жоғарғы мах жазбасы

және 74 сызықты емес мин төменгідей S блокпен жұмыс істейді. Бұл шифр криптотұрақты болуы мүмкін. Сәйкесінше кілт өлшемімен (128 бит) және өте жақсы шифрланады/дешифрланады. Өнімділігі: Мбайт 3,3 / с бойынша. 150 МГц Pentium процессоры.

Қорытынды.

Бұл мақалада ұсынылған CAST-128 шифры бүкіл әлемде қол жетімді, коммерциялық және коммерциялық емес. Осы құжатта сипатталған монолитті 128 шифр ұсынамыз, бүкіл әлемде қолжетімді коммерциялық және коммерциялық емес мақсаттар үшін тегін.

Қауіпсіздік мәселелері. Мұның бәрі қауіпсіздігі туралы, криптографиялық мақсаттар үшін арналған, өйткені онда арнайы алгоритм сипаттайды.

ӘДЕБИЕТ

- [1] [Adams] Adams, K., «Симметриялық шифрлер «құруда, CAST пайдаланады, Дизайндың тәртібі, кодтар конструкцияларында, және криптографиялық.
- [2] [Web1] «симметриялық алгоритмі құруда CAST Design Дизайн пайдаланылады.
- [3] «Petі ([Adams] ұқсас, бірақ онлайн қол жетімді) және» CAST
- [4] Дизайн тәртібі, «қосу <http://www.entrust.com/library.htm>
- [5] [Web2] «CAST шифрлау алгоритмі байланысты жарияланымдар» <http://adonis.ee.queensu.ca:8000/cast/cast.html>.
- [6] Диффи У., Хеллмен М. *Защищенность и имитостойкость. Введение в криптографию.* - ТИИЭР, 1976.- т. 67.- № 3.-71-109 сс.
- [7] Форузан Б.А. Криптография и безопасность сетей: учебное пособие / пер. с англ.; под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010. -784 с.
- [8] Нечаев В. И. Элементы криптографии (Основы теории защиты информации). - М.: Высшая школа, 1999. - 109 с.
- [9] Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. - М.: Гелиос АРВ, 2002. - 240 с.
- [10] Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая линия - Телеком, 2002. - 175 с. — (Специальность. Для высших учебных заведений).
- [11] Герасименко В. А. Защита информации в автоматизированных системах обработки данных., кн. 1, 2. М.: Энергоатомиздат, 1994.
- [12] Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996.
- [13] Конхейм А. Г. Основы криптографии. М.: Радио и связь, 1987.
- [14] Венбо Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. - М.: Вильямс, 2005. - 768 с.
- [15] Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
- [16] Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.
- [17] Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. СПб.: «Лань», 2000.
- [18] Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
- [19] Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004.
- [20] Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. 2-е изд. М.: Горячая линия - Телеком, 2013. - 229 с.
- [21] Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001.
- [22] Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.
- [23] Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. - М.: Диалектика, 2004. - 432 с.
- [24] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. - М.: Триумф, 2002. - 816 с.
- [25] Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.
- [26] Токарева Н. Н. Симметричная криптография. Краткий курс.

REFERENCES

- [1] [Adams] Adams, C., "Constructing Symmetric Ciphers using the CAST Design Procedure", Designs, Codes, and Cryptography (to appear).
- [2] [Web1] "Constructing Symmetric Ciphers using the CAST Design Procedure" (identical to [Adams] but available on-line) and "CAST Design Procedure Addendum", <http://www.entrust.com/library.htm>.
- [5] [Web2] "CAST Encryption Algorithm Related Publications", <http://adonis.ee.queensu.ca:8000/cast/cast.html>.
- [6] W. Diffie, Hellman M. Safety and infotouriste. An introduction to cryptography. TIER, 1976.- Т. 67. № 3.-71-109 SS.
- [7] Forouzan B. A. Cryptography and network security: a training manual / per. s angl.; edited by A. N. Berlin. М.: the Internet University of Information technologies: BINOM. Knowledge laboratory, 2010. 784 p.
- [8] V. I. Nechaev Elements of cryptography (fundamentals of the theory of information protection). М.: Higher school, 1999. 109 p.

- [9] A. V. Babash, Sankin G. P. the History of cryptography. Part I. Moscow: Gelios ARV, 2002. 240 p.
- [10] Borichev S. G., Goncharov V. V., Serov, R. E. foundations of modern cryptography. M.: Hot line - Telecom, 2002. — 175 p. (the Specialty. For higher education institutions).
- [11] Gerasimenko V. A. Protection of information in automated systems of data processing., kN. 1, 2. M.: Energoatomizdat, 1994.
- [12] the Basics of encryption ACS. Ed. by B. P. Kozlov. M: MO, 1996.
- [13] Konheim A. G. Fundamentals of cryptography. M.: Radio and communication, 1987.
- [14] Wenbo Mao. Modern cryptography. Theory and practice = Modern Cryptography: Theory and Practice. M.: Williams, 2005. 768 p
- [15] Mattick C. protection Mechanisms in computer networks. M.: Mir, 1993.
- [16] Melnikov V. V. Protection of information in computer systems. M.: Finance and statistics, 1997.
- [17] Construction Of A. A., Construction Of N. A. Advice B. Y. Cryptography. SPb.: "DOE", 2000.
- [18] Y. Romanets V., Timofeev P. A., Shangin V. F. Protection of information in computer systems and networks. M.: Radio and communication, 1999.
- [19] Ryabko B. Ya., Finow A. N. Basics of contemporary cryptography for specialists in information technologies. Moscow: Scientific world, 2004.
- [20] Ryabko B. Ya., Finow A. N. Cryptographic methods of information protection. 2nd ed. M.: Hot line Telecom, 2013. 229 p.
- [21] William Stallings. Cryptography and network security: principles and practice. M.; Williams, 2001.
- [22] Uhrinov L. M. Management of information security in automated systems. M.: MEFH, 1996.
- [23] Niels Ferguson, Bruce Schneier. Practical cryptography = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. M.: Dialectics, 2004. 432 p.
- [24] B. Schneier Applied cryptography. Protocols, algorithms, and source code in C = Applied Cryptography. Protocols, Algorithms and Source Code in C. M.: Triumph, 2002. 816 p.
- [25] V. V. Yashchenko an Introduction to cryptography. SPb.: Piter, 2001.
- [26] Tokareva N. N. Symmetric cryptography. Short course.

КРИПТОАНАЛИЗ СИСТЕМЫ ШИФРОВАНИЯ

А.М. Ахметова, С.А. Нугманова

Институт информационных и вычислительных технологии КН МОН РК, Алматы
КазНПУ им. Абая, Алматы

Ключевые слова: информационная безопасность, конфиденциальность информации, открытый ключ, секретный ключ, криптография с симметричными ключами, криптоанализ, интерпретация, инициализировать.

Аннотация. В современном мире информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности любого государства. Это, прежде всего, связано быстро растущими технологическими возможностями современных информационных систем. В работе рассматривается обзор и анализ существующих методов защиты информации криптографическим методом.

Шифрование с использованием ключа может помочь сохранить секреты в безопасности, но если нужно совместно использовать секретную информацию с другими людьми, необходимо также совместно использовать ключи. Но как безопасно отправлять ключи другим людям? В этой статье описаны некоторые решения, включая концепцию криптографии с ключом.

Чтобы решить задачу распределения ключей, можно использовать криптографию с ключом. В алгоритме данные, зашифрованные с помощью ключа, могут быть расшифрованы только с помощью секретного ключа. Только взаимодействующие стороны могут создать это секретное значение, которое затем будет использоваться в качестве сеансового ключа.

Каждый из трех алгоритмов имеет преимущества и недостатки, поэтому нельзя сказать, какой из них лучше, чем другие, алгоритм подбирается для конкретного применения.

Поступила 04.04.2016 г.

**Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

[www:nauka-nanrk.kz](http://www.nauka-nanrk.kz)

<http://www.physics-mathematics.kz>

Редактор *М. С. Ахметова*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 25.05.2016.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
10 п.л. Тираж 300. Заказ 3.