N E W S
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 encipherement 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 қауінсіздік, ақпараттың конфиденңиалдылығы, ашық кілт, құпия кілт, симметриялы кілті бар криптография, криптоанализ, иниңиализаңиялау, интерпретаңия.

Аннотация. Кілтті пайдалану арқылы шифрлау мәліметтердің қауінсіздігін сақтауға септігін тигізеді және ол басқа қолданушыға құпия ақпаратты білуге жол бермейді, сондай-ақ онымен қоса кілттерді пайдалануға болады. Бірақ басқа қолданушыға қалайша кілтті қауінсіз 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 алғоритмнің 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 неғізгі пайдалануды көздейді, кілт қалпына келтіру агентті пайдаланып кілттерді шифрлайды.

Кіріспе. Криптоанализ кілтімен байланысты, сызықты криптоанализ, шабуылга 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 сынга (SAC), Бит (БИК) сыныга 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 M1 ... M64; = K1 кілті K ... K128

Шыгыста: шифрленген мәтінді C1 ... C64.

1. (график кілті) К ден { КІІІ Кри } 16 жұп бөлімшесі есептелінеді.

2. (L0, r0) <- (M1 ... M64 (Сплит ашық мәтінін) солга, (L0 = M1 ... M32 и M33 R0 = ... m64). 32- разрядтың жартысы оңга

3. (16 тур) 1-ден 16-га дейінгі і үшін Li және Ri мынадай түрде келесі есептеледі Li = Ri-1;

Ri = L_{i-1} ^ F (R_{i-1}, K_{mi}, Кри), F -те анықталады. (F - 1тип, 2 типті немесе 3тип і-ге байланысты).

4. C1 ... C64 <- (R16, L16). (Қорытынды блоктар курсы L16, R16 және шифрленген мәтінді қалыптастыру, біріктіру). Жогарыда кетірілген шифрланган алгоритм шифрды ашу алгоритмімен бірдей, сонымен қатар ол (бөлімшелердің жұбы демек тізбектелген), (R16, L16) және (C0, R0) есептеу үшін кері тәртіппен пайдаланылады. Жасау үшін пайдаланылуы мүмкін тест векторлар В қосымшасында қараңыз. Осы алгоритмнің іске асыру дұрыстыгы.

Жұп кілттер раунды.

CAST-128 де бөлімшелердің жұбы раундта қолданылады: маска ретінде К.М пайдаланылады.

32 биттік сан болып табылады. «Кілті «айналу» Кр 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" ф и функциясы, деректердің кіріс "D"тиесілі). Назар аударыңыз,я гни«+»және «-» қосу және азайту 2 модулі бойынша ** 32, «^» А Биттік НЕМЕСЕ және «<<<» дөңгелек сол жақ болып табылады.

Жұмыс жалгасады.

Тип 1: Я = ((Kmi + D) <<< Кри)

F = ((S1 [IA] ^ S2 [Ib]) - S3 [Ic]) + S4 [ID]

Тип 2: Я = ((Kmi ^ D) <<< Кри)

F = ((S1 [IA] - S2 [Ib]) + S3 [Ic]) ^ S4 [ID]

Тип 3: Я = ((Kmi - Д) <<< Кри)

F = ((S1 [IA] + S2 [Ib]) ^ S3 [Ic]) - S4 [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, S5, S6, S7, S8 S-боксы функци ясы дөңгелектелген S-б Тек 4 Кбайт нақты шифрлеу кезінде қажетті екенін ескеріңіз оксы; және S1, S2, S3, S4 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. S1 - S8,S-блоктар. мазмұнына А қосымшасынан қараңыз.

Кілт кестесі

128-биттік кілт былай болса x0x1x2x3x4x5x6x7x8x9xAxBxCxDxExF,онда x0 ең үлкен байт XF ең маңызды байт болып табылады.

Былай болса, Z0..zF аралық болсын (уақытша) байт.

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

Кілт мына түйінен құралса x0x1x2x3x4x5x6x7x8x9xAxBxCxDxExF келесідей болады.

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

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

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

zCzDzEzF = x4x5x6x7 ^ S5 [ZA] ^ S6 [z9] ^ S7 [ZB] ^ S8 [Z8] ^ S6 [BP]
K25 = S5 [Z3] ^ S6 [Z2] ^ S7 [ZC] ^ S8 [ZD] ^ S5 [z9]
K26 = S5 [Z1] ^ S6 [z0] ^ S7 [ZE] ^ S8 [rP] ^ S6 [ZC]
K27 = S5 [Z7] ^ S6 [Z6] ^ S7 [Z8] ^ S8 [z9] ^ S7 [Z2]
K28 = S5 [Z5] ^ S6 [Z4] ^ S7 [ZA] ^ S8 [ZB] ^ S8 [Z6]
x0x1x2x3 = z8z9zAzB ^ S5 [Z5] ^ S6 [Z7] ^ S7 [Z4] ^ S8 [Z6] ^ S7 [z0]
x4x5x6x7 = z0z1z2z3 ^ S5 [x0] ^ S6 [x2] ^ S7 [x1] ^ S8 [x3] ^ S8 [Z2]
x8x9xAxB = z4z5z6z7 ^ S5 [x7] ^ S6 [x6] ^ S7 [x5] ^ S8 [x4] ^ S5 [Z1]
xCxDxExF = zCzDzEzF ^ S5 [xД] ^ S6 [x9] ^ S7 [BP] ^ S8 [x8] ^ S6 [z3]
K29 = S5 [x8] ^ S6 [x9] ^ S7 [x7] ^ S8 [x6] ^ S5 [x3]
K30 = S5 [xД] ^ S6 [BP] ^ S7 [x5] ^ S8 [x4] ^ S6 [x7]
K31 = S5 [xc] ^ S6 [XD] ^ S7 [x3] ^ S8 [x2] ^ S7 [x8]
K32 = S5 [xE] ^ S6 [XF] ^ S7 [x1] ^ S8 [x0] ^ S8 [XD]

Зерттеу нәтижесі.

Жасырынған бөлімдер және бұрмаланған бөлімдер.

Km1, ..., Km16 болса 32-разрядты жасырылган 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 = Ки; Кри = К16 + я; }

Айнымалы KeySize

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

8-бит қадаммен 40тан 128 битке өзгерілін отыруы мүмкін мөлшері, (Ягни, 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 (ягни, 40, 48, 56, 64-ге дейін
72 және 80 бит), нақты алгоритм сипатталган, 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.

Жогарыда, 40 бит, 64 бит, 80 бит және 128 бит, өлшемдері тиитік шартты қолдануды табу.

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

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

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

128-биттік кілт анық арналган, онда аты CAST5-128 пайдаланылган тиіс.

CAST5 нысана идентификаторы.

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

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 ұзындыгы бүтін сан – кілт ұзындыгы }

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

Болмауга тиіс, IV егер барлық нөлдерді пайдаланганда кодтау соңында.

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

CBC режимінде бұл шифрлеу және дешифрлеу симметриялық алғоритм блок шифры.

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

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

Кілттің ұзындығы бүтін сан- бит негізгі ұзындығы}

Симметриялық блок Cast-128 шифрлау алғоритмі пайдаланылған хабар аутентификаңиясы.

pbeWithMD5AndCast5CBC идентификатор нысаны :: =

Параметрі:: = тізбектелген {Октетов жол

iterationCount сан, хэш - итераңияларының жалпы саны –

Кілттің ұзындығы бүтін сан- бит негізгі ұзындығы}

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

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

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

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

Холост жинақтары Plaintext-Key -шифрланған мәтін

Алғоритм 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 а және Ь 128-биттік векторлар болып табылады тиіс, Al және AP сол және оң жартысы болады, BL және BR сол және оң жартысы б және шифр (D, K) болады шифрлау режимінде ECB

Блокта D кілтті асты К. шифрлау болып табылады.

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

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

1000000 рет істеу

{ аЬ = шифрлеу (Al, б)

AR = шифрлеу (Ar, б)

BL = шифрлеу (BL, а)

Марка = шифрлеу (Марка, а)}

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

Көз жеткізідік, б == 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 дифференңиалдық ішінен шабуылдарға тұрақты пайдаланады. Қоспасы функңиясы (**) 32 бойынша 2 модулі XOR, қосу және азайтуды қолданылады; және шифрлау кезеңінде функңияның үш фазалы өзгермелілігі түрленуі пайдаланады. Соңында, 8х32 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.

Қауінсіздік мәселелері. Мұныц бәрі қауінсіздігі туралы, криптоғрафиялық мақсаттар үшін арналған, өйткені онда арнайы алғоритм сипаттайды.

ӘДЕБИЕТ

[1] [Адамс] Адамс, К., «Симметриялық шифрлер «құруда, CAST пайдаланады, Дизайнның тәртібі, кодтар конструкцияларында, және криптографиялық.

[2] [Web1] «симметриялық алгоритмі құруда CAST Design Дизайн пайдаланылады.

[3] «Реті ([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] Фороузан 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

[3] Procedure" (identical to [Adams] but available on-line) and "CAST

[4] 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.- T. 67. № 3.-71-109 SS.

[7] Forouzan B. A. Cryptography and network security: a training manual / per. s angl.; edited by A. N. Berlin. M.: 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). M.: 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.: MEPhI, 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, интрпретация, 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.