UYALI ALOQA TIZIMI GSM STANDARTIDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING KRIPTOGRAFIK JIHATLARI

Alimardonov Shohruh Erkin o'g'li
O'zbekiston Respublikasi Mudofaa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti Radioelektron razvedka va kurash kafedrasi kursant

***Annotatsiya**: Ushbu maqolada uyali aloqa tizimida keng tarqalgan GSM standarti va unda ma'lumotlar xavfsizligini ta'minlash tizimi, GSM standartida foydalaniladigan shifrlash algoritmlari va ularning kriptografik asoslari keltirilgan.*

***Kalit so'zlar**: uyali aloqa tizimi, GSM standarti, abonent terminali, bazaviy stansiya, autentifikatsiya, autentifikatsiya markazi, shifrlash algoritmi, kriptokalit, shifr matn, ochiq matn, registr, takt boshqaruvi.*

***Аннотация**: В данной статье описывается стандарт GSM и его система защиты данных, алгоритмы шифрования, используемые в стандарте GSM, и их криптографическая основа, которые широко используются в системах мобильной связи.*

***Ключевые слова**: система мобильной связи, стандарт GSM, абонентский терминал, базовая станция, аутентификация, центр аутентификации, алгоритм шифрования, криптовалюта, зашифрованный текст, открытый текст, регистр, управление тактами.*

***Abstract**: This article describes the GSM standard and its data protection system, encryption algorithms used in the GSM standard and their cryptographic basis, which are widely used in mobile communication systems.*

***Keywords: mobile** communication system, GSM standard, subscriber terminal, base station, authentication, authentication center, encryption algorithm, cryptocurrency, cipher text, plain text, register, tact control.*

Uyali aloqa tiziming ikkinchi avlodi hisoblanadigan GSM standarti 1991-yilda Yevropa telekommunikatsiya standartlari instituti tomonidan taklif etilgan va shu yilning o'zida Yevropaning 17 davlatida umumiy uyali aloqa standarti sifatida qabul qilingan. Hozirgi vaqtda GSM tizimi qamrovi va obunachilari soni bo'yicha dunyoda yetakchi o'rinni egallaydi. Shu jihatdan ushbu standartda foydalanuvchilarning ma'lumotlari xavfsizligini ta'minlash, tarmoqqa noqonuniy ulanish, qonunga xilof ravishda tarmoq hosil qilish va abonentlarning huquqlarini

buzishni oldini olish doimiy e'tibor qaratilish zarur masala hisoblanadi [2].

Abonentlarning ma'lumotlari xavfsizligi ta'minlash uchun GSM standartida xavfsizlik tizimi joriy etilgan bo'lib, u 3 algoritm asosida tashkil etiladi:

A3 — autentifikatsiya algoritmi;

A8 — kriptokalit generatsiyasi algoritmi;

A5 — bazaviy stansiya bilan abonent terminali o'rtasidagi ma'lumot maxfiyligini ta'minlovchi raqamli nutq shifrlash algoritmi [3].

A3 va A8 algoritmlari abonent terminalida joylashtiriladigan sim – karta orqali amalga oshiriladi, abonent terminali (telefon) da A5 algoritmiga ega ASIC chipi mavjud bo'ladi. Bazaviy stansiyalar ham A5 algoritmiga ega ASIC chipi va mobil abonentini aniqlash va sessiya kalitini yaratish uchun A3, A5, A8 algoritmlaridan foydalanadigan autentifikatsiya markazi bilan jihozlanadi [6].

GSM standartida xavfsizlik tizimi quyidagi tartibda ishlaydi. Uyali aloqa abonent terminali bazaviy stansiya orqali umumiy tarmoqqa ulanadi. Bunda abonent terminali bazaviy stansiyaga o'zining haqiqiyligini ta'minlash uchun autentifikatsiya jarayoni amalga oshiriladi, ya'ni bazaviy stansiya 128 bitli tasodifiy bitlar hosil qilib abonent terminaliga uzatadi. Abonent terminali qabul qilingan 128 bitli sonli ketmaketlikni A3 algoritmi va autentifikatsiy akaliti yordamida shifrlaydi. Hosil bo'lgan shifr matnning 32 bitini olib, autentifikatsiya markaziga uzatadi. Autetifikatsiya markazida ham shu jarayon bo'ladi. Faqat . autetifikatsiya markazi o'zida hosil bo'lgan va abonent terminalidan kelgan shifrmatnlarni o'zaro solishtiradi. Agar shifr matnlar o'zaro teng bo'lsa abonent haqiqiy deb topiladi [6].

Keyingi bosqichda abonentning aloqa o'rnatishi uchun A8 algoritmi yordamida 64 bitli sessiya kaliti hosil qilinadi va A5 algoritmi orqali aloqa vaqtida davomida ma'lumotlar shifrlanadi.

Ovozli ma'lumotlar xavfsizligi A5 oqimli shifrlash algoritmi orqali amalga oshirilib, bugungi kunda A5 oilasiga mansub 3ta shifrlash algoritmi mavjud:

A5/1 – oqimli shifrlash, bugungi kunda eng ko'p tarqalgan turi.

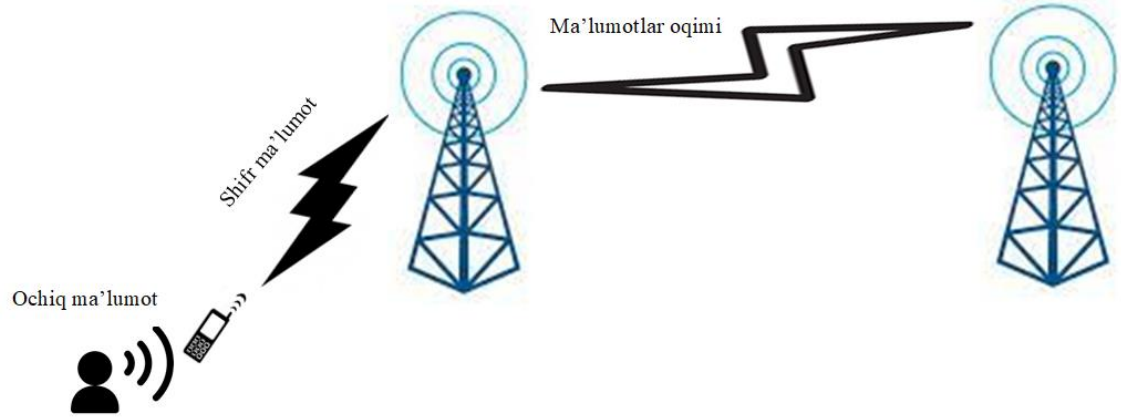
A5/2 – oldingi shifrlash algoritmining varianti bo'lib, u A5/1 ga juda o'xshaydi, lekin A5/1 ning juda zaiflashgan versiyasi sifatida o'ylab topilgan.

A5/3 – blokli shifrlash turi bo'lib, eskirgan A5/1 algoritmini almashtirish uchun 2002 – yilda ishlab chiqilgan. Biroq, hozirda u faqat 3GPP tarmoqlarida ishlatiladi.

Algoritmda bir qancha zaifliklar topilgan, lekin amaliy hujumlar haqida hozircha aniq ma’lumotlar mavjud emas [4].

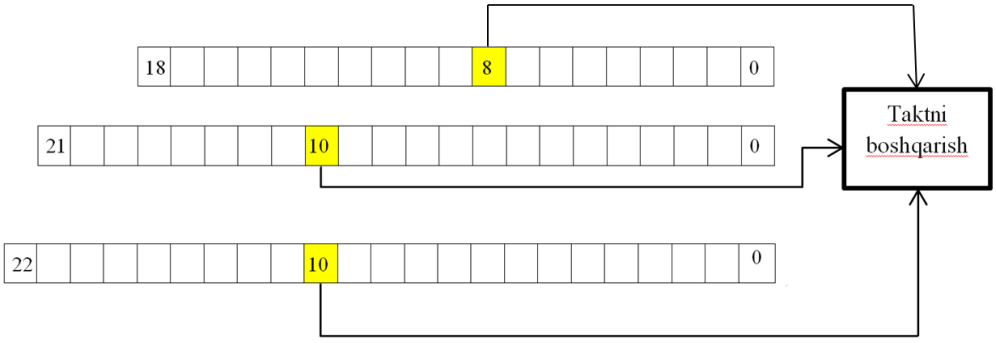
A5 shifrlash algoritm oilasida A5/1 oqimli shifrlash algoritmi GSM standartining xavfsilik tizimida alohida o‘ringa ega bo‘lib, quyida ushbu algoritmga to‘xtalamiz.

A5/1 oqimli shifrlash algoritmi bo‘lib, GSM standartida mobil qurilma bilan bazaviy stansiya o‘rtasida ma’lumot maxfiylilgini ta’minlab beradi.



1-rasm. Uyali aloqa tizimida ochiq va yopiq ma’lumotlarni uzatish

A5/1 oqimli shifrlash algoritmida psevdotasodifiylik 3 siljish registri (R1, R2, R3) orqali amalga oshiriladi. Siljish registrlari mos ravishda 19, 22 va 23 bitli o‘lchamda (umumiy 64 bit) bo‘ladi. Registlardagi siljishlar ma’lum funksiya (*majority* deb ham ataladi: $(a_1, a_2, a_3) = a_1a_2 \vee a_2a_3 \vee a_1a_3$) – har bir registrda nazorat biti mavjud: birinchi registrda 8-bit (a_1), ikkinchi va uchinchi registrda 10-bit (a_2 va a_3) [3].

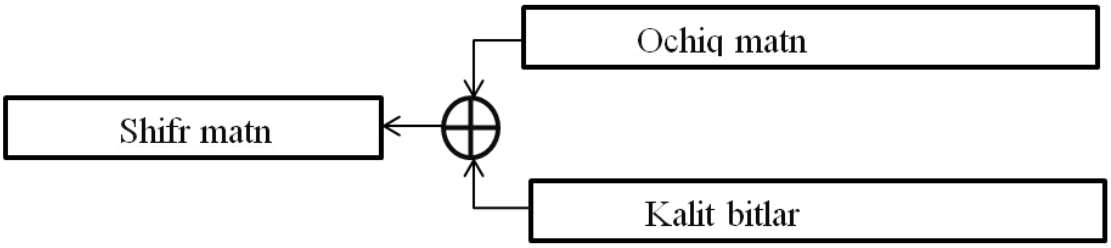


2-rasm. A5/1 oqimli shifrlash algoritmida siljish registrlarida takt boshqaruvi

Bitlar o‘ngdan chapga raqamlanadi. Navbatdagi taktda m funksiyaning holatiga mos keladigan registlar holati o‘zgartiriladi. Siljishni boshqarish funksiyasi va $m(a_1, a_2, a_3)$ quyidagicha o‘zaro bog‘langan:

$$c(x) = (a_1 \equiv m, a_2 \equiv m, a_3 \equiv m). \quad (1)$$

Registlarning oxirgi bitlari 2 modul bo‘yicha yig‘indisi hisoblanadi. Yig‘indi natijasi yangi γ bitni hosil qiladi. γ bit ochiq matnga qo‘shiladi va shifr matn hosil qilinadi. Bir kalitda 114 bit γ hosil qilinadi [6].

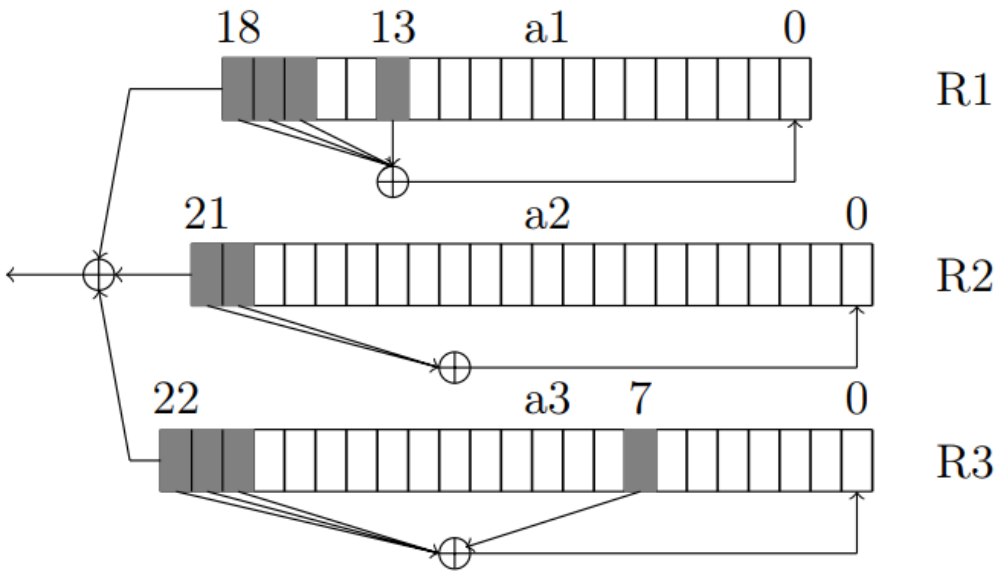


3-rasm. A5/1 oqimli shifrlash algoritmida shifrmatnni hosil qilish tartibi

Chiziqli teskari aloqa funktsiyalarini polinomlar orqali ifodalash qulay bo‘lib, registrning har bir bitiga x o‘zgaruvchining mos keladigan darajasini belgilash orqali amalga oshiriladi. A5/1 shifrida teskari aloqa funktsiyalari o'rnatiladi quyidagi polinomlar bo‘yicha ifodalanadi [3]:

$$\begin{aligned} &x^{19} + x^{18} + x^{17} + x^{14} + 1 && \text{R1 uchun} \\ &x^{22} + x^{21} + 1 && \text{R2 uchun} \\ &x^{23} + x^{22} + x^{21} + x^{8} + 1 && \text{R3 uchun} \end{aligned} \quad (2)$$

Misol uchun registrda 18-, 17-,16- va 13-raqamli bitlar yig‘indisi hisoblanadi va natija o‘ng chetki biti uchun yangi qiymat sifatida qabul qilinadi.



4-rasm. Psevdotasodifiylikni ta’minlashda siljish registrlarida bitlarning siljishi

Algoritmni ishga tushirishdan ma’lumotlar 114 bitli kadrlarga bo‘linadi, so‘ng registrlar quyidagi tartibda ishga tushiriladi:

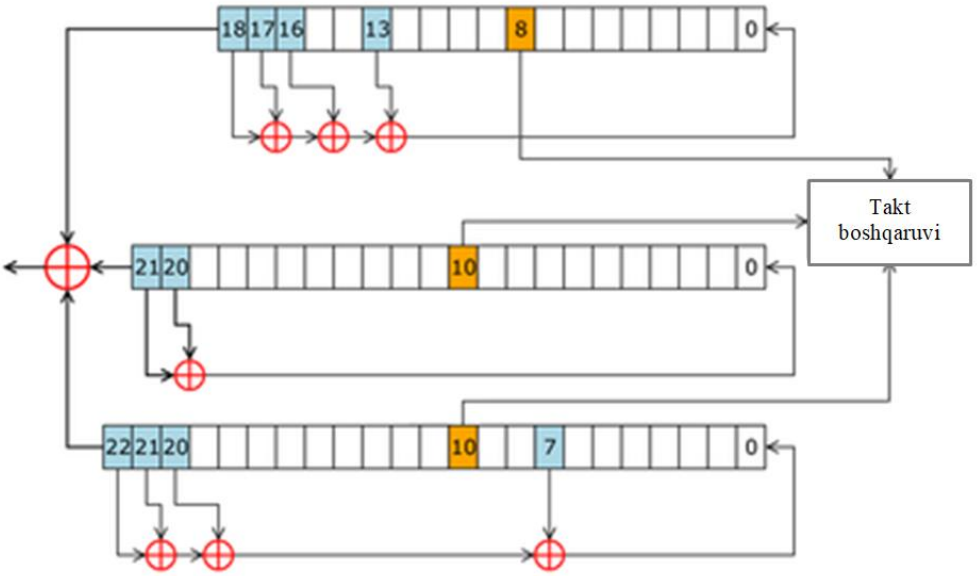
1. R1=R2=R3=0 ya’ni registlarga nol (0) lar yuklanadi.

2. Algoritm kirishiga A8 algoritmi orqali hosil qilingan seans kaliti va kadr raqami kiritiladi.

3. Initsializatsiya jarayonida 64 takt davomida kalitning navbatdagi biti registrning kichik biti bilan XOR – lanadi va har bir taktda registlrada siljish amalga oshiriladi. Keyingi 22 taktda XOR amali kadr raqami bilan bajariladi. 100 taktda registrlar siljishi boshqariladi.

4. 228 bitli (114+114) taktda uzatiladigan ma’lumotlar (114 bit) shifrlanadi va qabul qilingan ma’lumotlar (114 bit) deshifrlanadi.

5. Initsializatsiya jarayoni qaytadan boshlanadi va yangi kadr raqamidan foydalaniladi [6].



5-rasm. A 5/1 algoritmi umumiy chizmasi

	A5/1	A5/2	A5/3

Xulosa

Har qanday aloqa tizimida ham ma’lumotlar xavfsizligini ta’minlash birinchi navbatda turadi. Shu jihatdan aloqa tizimida ma’lumotlarni shifrlash, autentifikatsiya va identifikatsiyalash jarayonlari muhim omil hisoblanadi. Ushbu masalalar ham GSM standartida muhim ahamiyatga ega.

GSM standartining ishlab chiqilishida buzib bo‘lmaydigan (ayniqsa real vaqtda) kuchli shifrlash apparati maqsad qilingan. Amalga oshirilgan ishlanmalar, to‘g‘ri bajarilgan holda, uzatilgan ma’lumotlarning yuqori sifatli shifrlanishini ta’minladi. GSM standartida oqimli shifr algoritm qo‘llanilishi real vaqtda kriptokalitni topish, shifr matnni deshifrlash va ma’lumotlarni ruxsatsiz olish imkonini bermaydi. Lekin so‘nggi vaqtlarda ma’lumotlarni noqonuniy olish usullarining ko‘payishi, zamonaviy texnologiyalarning rivojlanishi GSM standartida ham ma’lumotlarni olish, qayta tiklash imkonini bermoqda.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Telekommunikatsiyalar to‘g‘risida” gi Qonuni, №822, 1999 yil 20 avgust.

2. О сокращении ключевого пространства шифра a5/1 и обратимости функции следующего состояния в поточном генераторе, С.А.Кисел¨ев, Н.Н.Токарева, “Дискретный анализ и исследование операций” Март-апрель 2011. Том 18, № 2. С. 51–63.

3. Сети и стандарты мобильной связи, Данилов В. И., учебное пособие, Санкт-Петербург 2015 г., С.19-47.

4. Системы подвижной радиосвязи, Кшиштоф Веселовский, М.: Горячая линия – Телеком, 2006 г.

5. https://ru.wikipedia.org/wiki/A5_(алгоритм_шифрования).

6. https://habr.com/ru/Безопасность GSM сетей: шифрование данных.