# SM4 SHIFRLASH ALGORITMINI DASTURIY AMALGA OSHIRISH USULLARI

**I.S.Olimov**

[1]Tashkent university of information technologies named after Muhammad al- Khwarizmi

E-mail: iskandar.olimov@mail.ru

***Annotatsiya.*** *Ushbu maqolada SM4 shifrlash algoritmini dasturiy amalga oshirish usullariga bag‘ishlangan bo‘lib, SM4 shifrlash algoritmi haqida umumiy tasnif, uni dasturiy amalga oshirish usullari batafsil yoritilgan undan tashqari ularni tahlili amalga oshirilgan.*

***Kalit so‘zlar.*** *SM4, C, C++, Java, Python, OpenSSL, Bouncy Castle, Crypto++.*

## Kirish

SMS4 nomi bilan ham tanilgan SM4 shifr 2007 yilda Xitoy Milliy Kriptografiya Byurosi (NCB) tadqiqotchilari tomonidan ishlab chiqilgan. U Xitoy uchun ma’lumotlar maxfiyligini ta’minlashda foydanilgan shifrlash standarti DES va uning vorisi o‘rnini bosuvchi milliy standart shifrlash algoritmi sifatida ishlab chiqilgan.

SM4 ni ishlab chiqishni Davlat Kriptografiya Boshqarmasidagi professor Lai Xuejia va uning jamoasi ishlab chiqan. Ularni asosiy maqsadi Xitoyda turli ilovalar, jumladan xavfsiz aloqa, ma’lumotlarni himoya qilish va moliyaviy operatsiyalar uchun keng qo‘llanilishi mumkin bo‘lgan xavfsiz va samarali shifrlash algoritmini yaratish bo‘lgan.

SM4 shifrining xavfsizligini ta’minlash uchun jiddiy tahlil va baholashdan o‘tkazildi. Dizayn jarayoni matematik tahlil, kriptografik tadqiqotlar va keng qamrovli testlarni o‘z ichiga olgan. Algoritm ma’lum hujumlarga qarshi kuchini

tekshirish uchun differensial kriptotahlil va chiziqli kriptoanaliz kabi bir qator kriptotahlil usullaridan o‘tkazildi [5,8].

Turli baholash bosqichlaridan muvaffaqiyatli o‘tgandan so‘ng, SM4 2012 yilda Xitoyda milliy standart sifatida rasman e’lon qilindi. U SCA tomonidan Xitoydagi davlat idoralari, moliya institutlari va boshqa tashkilotlar uchun tavsiya etilgan simmetrik shifrlash algoritmi sifatida qabul qilindi. U mamlakat kriptografik hamjamiyatida keng tan olingan va qabul qilingan algoritm bo‘ldi.

SM4 asosan Xitoyda qo‘llanilsada, u xalqaro e’tibor va e’tirofga sazovor bo‘ldi. 2012 yilda SM4 ISO/IEC 18033-3 xalqaro standartiga blokli shifrlar uchun profil sifatida kiritilgan, ya’ni u ushbu standartga mos keladigan kriptografik protokollarda qurilish bloki sifatida ishlatilishi mumkin bo‘ldi.

SM4 shifrlash algoritmini dasturiy amalga oshirish usullari

SMS4 algoritmi sifatida ham tanilgan SM4 shifrlash algoritmi ma’lumotlarni shifrlash va shifrini ochish uchun ishlatiladigan simmetrik blokli shifrdir. Bu Xitoyda keng tarqalgan bo‘lib qabul qilingan standart bo‘lib, turli ilovalarda, jumladan xavfsiz aloqa va ma’lumotlarni himoya qilishda qo‘llaniladi. Bu yerda SM4 algoritmining apparat va dasturiy ta’minotni amalga oshirish jihatlari haqida umumiy ma’lumot keltirilgan:

*Dasturlash tillari:* SM4 C, C++, Java yoki Python kabi turli dasturlash tillarida amalga oshirilishi mumkin. Tilni tanlash maqsadli platforma, ishlash talablari va ishlab chiquvchining afzalliklariga bog‘liq.

*Kriptografik kutubxonalar:* OpenSSL, Bouncy Castle yoki Crypto++ kabi kriptografik kutubxonalar SM4 shifrlash va ochiq matnga qaytishni amalga oshirish uchun oldindan tuzilgan funksiyalar va API-larni taqdim etadi. Ushbu kutubxonalar past darajadagi kriptografik operatsiyalarni boshqaradi va ishlab chiquvchilar uchun SM4 ni o‘zlarining dasturiy ilovalariga osongina integratsiya qilish uchun interfeysni taqdim etadi.

*Operatsion tizimni qo‘llab-quvvatlash:* SM4 ilovalari turli xil operatsion tizimlarda, jumladan Windows, Linux, macOS va RTOS (Real-Time Operating Systems) kabi o‘rnatilgan tizimlarda ishlash uchun ishlab chiqilishi mumkin.

*Ilovalar bilan integratsiya*: SM4 ilovalari xavfsiz xabar almashish ilovalari, VPNlar, fayllarni shifrlash dasturlari yoki tarmoq xavfsizligi vositalari kabi turli ilovalarga birlashtirilishi mumkin [1,2,5].

**SM4 shifrlash algoritmiga qo‘yilgan xavfsizlik talablari**

Shuni ta’kidlash kerakki, SM4 kabi kriptografik algoritmlarni qo‘llashda xavfsiz kodlash, kalitlarni boshqarish va algoritm konfiguratsiyasi uchun o‘rnatilgan eng yaxshi amaliyotlarga amal qilish juda muhimdir. Bundan tashqari, amalga oshirishda aniqlanishi mumkin bo‘lgan har qanday zaiflik yoki zaifliklarni bartaraf etish uchun muntazam xavfsizlik talablarini oshirish kerak.

SM4 simmetrik blokli shifrlash algoritmi bo‘lib, Xitoy standart shifrlash algoritmi bo‘lib, tuzilishi va ishlashi jihatidan AES (Advanced Encryption Standard) algoritmiga o‘xshaydi. SM4 shifrlash yoki har qanday blokli shifrlash algoritmini tahlil qilishda odatda bir nechta jihatlar hisobga olinadi:

*Xavfsizlik:* Kriptografik algoritmlar turli xil hujumlarga chidamliligiga qarab baholanadi. SM4 xavfsizligi kriptografik hamjamiyat tomonidan keng tahlil qilingan. U ma’lum hujumlarga, shu jumladan differentsial va chiziqli kriptoanalizga qarshi chidamliligini ta’minlash uchun jiddiy tekshiruv va baholashdan o‘tdi.

*Asosiy quvvat:* SM4 bilan ishlatiladigan shifrlash kalitining kuchi uning xavfsizligi uchun juda muhimdir. Shuning uchun 128 bit uzunlikdagi kalit tavsiya etiladi.

*Ishlash tartibi:* SM4 ham boshqa blokli shifrlash algoritmlari kabi Elektron Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR) yoki Galois/Counter Mode (GCM) rejimlar bilan birgalikda ishlatiladi.

*Amalga oshirish:* Algoritmning amalda bajarilishi juda muhim. Algoritmning to‘g‘ri va xavfsiz ishlashini ta’minlash uchun u eng yaxshi amaliyotlar va xavfsizlik ko‘rsatmalariga amal qilishi kerak [4,6].

*Kriptanaliz:* Kriptanaliz - bu zaif yoki zaif tomonlarni topish maqsadida kriptografik algoritmlarni o‘rganishdir. *Kriptonalistlar* SM4 kabi algoritmlarni tahlil qilib, potentsial hujumlar yoki ularning xavfsizligiga putur etkazadigan kamchiliklarni aniqlaydilar.

**SM4 shifrlash algoritmini kutubxona va dasturlash tillari bilan ishlashi**

SM4 shifrlash yoki har qanday blokli shifrlash algoritmini tahlil qilishda ushbu omillarni hisobga olish va tegishli tadqiqot hujjatlari, kriptografik standartlar va professional kriptograflarning tajribasi bilan maslahatlashish zarur. Bundan tashqari, kriptografiya sohasidagi so‘nggi ishlanmalar va yutuqlardan xabardor bo‘lish talab etiladi.

*SM4:*

*Maqsad:* SM4 simmetrik blokli shifrlash algoritmi bo‘lib, ma’lumotlarni shifrlash va shifrini ochish uchun ishlatiladi.

*Kalit uzunligi*: 128 bit

*Blok uzunligi*: 128 bit

*Ishlash tartibi*: SM4 turli xil ish rejimlarini, jumladan, ECB (Elektron kod kitobi), CBC (Cipher Block Chaining) va boshqalarni qo‘llab-quvvatlaydi.

*Xavfsizlik:* SM4 ma’lum hujumlardan himoyalanish uchun mo‘ljallangan va tavsiya etilgan kalit uzunliklari bilan foydalanilganda kuchli shifrlashni ta’minlaydi.

Shuni ta’kidlash kerakki, ushbu algoritmlar Xitoy Milliy Kriptografik Algoritm To‘plamining (CNSA) bir qismidir va Xitoyda keng qo‘llaniladi. Ular kriptografik hamjamiyat tomonidan keng qamrovli tahlil va baholashdan o‘tdi. Biroq, har doim eng so‘nggi ishlanmalardan xabardor bo‘lib turish va ushbu algoritmlarni real dunyo ilovalarida amalga oshirishda tavsiya etilgan eng yaxshi amaliyotlardan foydalanish tavsiya etiladi [3,7].

SM4 shifrlash algoritmini ishlashi ba’zi kutubxona va dasturlash tillari orqali taqqoslash jadvali:

1-jadval

**SM4 shifrlash algoritmi**

| *Amalga oshirish* | *Dasturlash tili* | *Xususiyatlari* |
|---|---|---|
| OpenSSL | C | SM4 qo‘llab-quvvatlashi bilan keng qo‘llaniladigan kriptografik kutubxona. Shifrlash funksiyalari va turli xil shifrlash rejimlarini qo‘llab-quvvatlaydi |
| Bouncy Castle | Java | SM4 qo‘llab-quvvatlaydigan keng qamrovli kriptografik kutubxona. Oson integratsiya uchun yuqori darajadagi API-larni taklif qiladi va bir nechta platformalarni qo‘llab-quvvatlaydi. |
| Botan | C++ | SM4 qo‘llab-quvvatlanadigan samarali kriptografik kutubxona. Shifrlash uchun API taqdim etadi va bir nechta shifrlash rejimlarini qo‘llab-quvvatlaydi. |
| PyCryptodome | Python | SM4 qo‘llab-quvvatlanadigan Python kutubxonasi. Nosimmetrik shifrlash uchun yuqori darajadagi API’larni, jumladan, SM4ni va boshqa kriptografik funksiyalarni taklif qiladi. |
| Cryptlib | C | SM4 qo‘llab-quvvatlaydigan. Shifrlash uchun ishlatish qulay API-larni taqdim etadi va bir nechta platformalarni qo‘llab-quvvatlaydi. |

**Xulosa**

Xulosa qilib aytganda, SM4 blokli shifrlash algoritmi feystal tarmog‘iga asosolangan bo‘lib, ma’lumotlarni maxfiyligini ta’minlashda foydaniladigan algoritm hisoblanadi. Ushbu maqoladi SM4 shifrlash algoritmi haqida umumiy tushuncha,

unga qo‘yilgan xavfsizlik talablari, bu algoritmni dasturiy amalga oshirish usullari va ularni tahlili keltirilgan.

**Foydalangan adabiyotlar ro‘yxati**

1. Olimov I.S., Ortiqboyev A.M., “Buyumlar internetining (Internet of things, IOT) Arxitekturasi va xavfsizlik muammolari”. Axborot kommunikatsiyalari: Tarmoqlar, Texnologiyalar, Yechimlar. №2 (54). Toshkent-2020. -B. 32-41.

2. Boriyev Y.A., Sadikov M.A., Khamidov SH.J., “Internet of things architecture and security challenges ICISCT 2020 confrence international conferencye on information sciyencye and communications technologiyes 4,5,6 November.

3. Abed, Sa’ed, et al. "Performance evaluation of the SM4 cipher based on field-programmable gate array implementation." *IET Circuits, Devices & Systems* 15.2 (2021): 121-135.

4. Rao, J., & Cui, Z. (2022). Chosen Plaintext Combined Attack against SM4 Algorithm. *Applied Sciences*, *12*(18), 9349.

5. Zhou, Y., Wu, N., Hu, B., Zhang, Y., Qiu, J., & Cai, W. (2022). Implementation and Performance of Face Recognition Payment System Securely Encrypted by SM4 Algorithm. *Information*, *13*(7), 316.

6. Zhou, Y., Wu, N., Hu, B., Zhang, Y., Qiu, J., & Cai, W. (2022). Implementation and Performance of Face Recognition Payment System Securely Encrypted by SM4 Algorithm. *Information*, *13*(7), 316.

7. Li, Y., Wu, X., & Bai, G. (2018, October). Implementation of SM4 Algorithm based on Asynchronous Dual-Rail Low-power Design. In *2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)* (pp. 1-3). IEEE.

8. Chen, Rui, and Bing Li. "Exploration of the High-Efficiency Hardware Architecture of SM4-CCM for IoT Applications." *Electronics* 11, no. 6 (2022): 935.