INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.4 №4 (2026). April
innovativepublication.uz

OneTimePad shifrlash algoritmi. Buzib bo‘lmas shifrlashning ishlash prinsipi

RASHIDOVA OYDINOY JO‘RABEK QIZI
TATU akademik litseyi o‘quvchisi
MAXMUDOV ABDUAZIM MUZAFFAR O‘G‘LI
TATU akademik litseyi o‘quvchisi

Annotatsiya: Ushbu maqolada klassik kriptografiyaning ikkita asosiy ustuni — Vijenyer shifri va OneTime Pad algoritmlari qiyosiy tahlil qilinadi. Tadqiqotning asosiy maqsadi ushbu algoritmlarning kalit generatsiya qilish tamoyillari va ularning buzilish usullari o‘rtasidagi farqlarni yoritishdir. Tadqiqot natijalari shuni ko‘rsatadiki, zamonaviy axborot xavfsizligida shifrlash algoritmining o‘zigina emas, balki kalitning tasodifiyligi va bir martalik qo‘llanilishi hal qiluvchi ahamiyatga ega.
Kalit so‘zlar: *Vijener shifri, OneTimePad, XOR amali, Kasiski testi, Venona loyihasi, kalit generatsiyasi.*

The One-Time Pad Encryption Algorithm: Principles of Unbreakable Cryptography

RASHIDOVA OYDINOY JORABEK QIZI
Student at the Academic Lyceum of Tashkent University of Information Technologies (TUIT)

Abstract: This paper presents a comparative analysis of two fundamental pillars of classical cryptography: the Vigenère cipher and the One-Time Pad (OTP) algorithm. The primary objective of the study is to highlight the differences between their key generation principles and their respective cryptanalysis methods. The research findings demonstrate that in the context of modern information security, the effectiveness of encryption depends not solely on the algorithm itself, but critically on the randomness and single-use nature of the key.
Keywords: *Vigenère cipher, One-Time Pad, XOR operation, Kasiski examination, Venona project, key generation.*

Kirish

Kriptografiya tarixida inson tomonidan doimo mukammal shifrlash algoritmini yaratishga intilib kelingan. RSA algoritmi tub sonlar va faktorlash muammosiga asoslangan murakkab shifrlash algoritmi hisoblansa ham,uni buzish mumkin. Kalit ochiq holatda beriladi.AES ham hisoblash murakkabligiga ega hisoblanadi. Bu kabi algoritmlarni nazariy holatda buzish mumkin.

1917-yilda Gilbert Vernam tomonidan yaratilgan va mayor J.Maugborn tomonidan taklif qilingan simmetrik shifrlash algoritmida shifrni ochish va shifrlash uchun ayni bir kalit ishlatiladi. 1882-yilgi Frank Miller ham birinchilardan bo‘lib, o‘z ishlarida OneTimePad haqida g‘oyalar bergan[2].

OneTimePad shifrlash zamonaviy shifrlashga ajoyib pedagogik kirishni taqdim etadi. Lekin zamonaviy shifrlashda amaliy jihatdan kamdan-kam qo‘llaniladi. Aksariyat

zamonaviy oqim shifrlashlarida esa OneTimePad bir martalik shifrlash simulyatsiyasi hisoblanadi[2].

Metodlar

OneTimePad shifrlash algoritmini ishlash prinsipida quyidagi shartlar bajarilishi kerak:

a) Kalit-ochiq matn bilan bir xil uzunlikda bo‘lishi kerak.

b) Tasodifiy-berilgan kalit haqiqatda tasodifiy sonlar tashkil topgan bo‘lishi kerak.

c) Bir martalik-Bu shifrlash usulining nozik joyi. Shuning uchun ishlatilgan kalitni qayta ishlatmaslik zarur.

Matematik jihatdan olib qaraganda algoritm XOR mantiqiy amali yordamida bajariladi.

$$C = P \oplus K$$

C-shifrlangan matn, P-ochiq matn, K -kalit.

Endi shifrdan ochishga qarasak, unda yana shu amal bajariladi:

$$P = C \oplus K$$

Bu yerda oddiy mantiqiy amallar yotibdi.

$$P = C \oplus K = (P \oplus K) \oplus K = P \oplus (K \oplus K) = P \oplus 0 = P$$

XOR amali o‘zi qanday ishlaydi degan savolga javob oddiy. Uni quyida jadvaldan ko‘rish mumkin.

A	B	$A \oplus B$
0	1	1
0	0	0
1	1	0
1	0	1

Vijener shifrlash algoritmi va OneTimePad orasida o‘xshashlik bordek tuyuladi.Aslida esa unday emas. Vijener shifrlashida ham, OneTimePad ning umumiy ko‘rinishida ham bir xil shifrlash va shifrdan ochish algoritmi qo‘llaniladi:

$$C_i = (P_i + K_i)\ mod\ 26$$

C_i-i-indeksdagi shifrmatn, P_i – i-indeksdagi ochiq matn va K_i- i-indeksdagi kalit. 26 soni lotin alifbosida 26 ta harf bo‘lgani uchun.

Natijalar

Agar kimdir shifrlangan matnni topib olsa, u barcha ehtimoliy kalitlarni sinab ko‘rishi kerak. Vijener va OneTimePad ning farqli joyi, kalit generatsiya qilishda. Vijener da kalit uzunligi yetarli bo‘lmasa, takrorlash mumkin. OneTimePadda buni iloji yo‘q. Uning buzilmasligi kalitni takrorlanmasligida .

Albatta, zamonaviy OneTimePad da XOR amali bajariladi, lekin klassik shifrlash davrida uning o‘rniga Vijener algoritmidagidek shifrlash usuli ishlatilgan.

Vijener shifrlash algoritmini 19 asrda Fridrix Kasiski birinchilardan buzib ko‘rgan. Undan keyin 20 asr boshlarida Uilyam Fridman uni matematik statistika bilan chastotalarni o‘lchash orqali buzishni taklif qildi va bu Kasiski testidan aniqroq edi.

OneTimePad algoritmi buzilishi Ikkinchi jahon urushi davriga to‘g‘ri keladi.

Sovet Ittifoqi Ikkinchi jahon urushi davrida kalitlar tanqisligi tufayli ba'zi OTP kalitlarini qayta ishlatgan. AQSh va Britaniya kriptoanaliz (Venona loyihasi) aynan shu xatolikdan foydalanib, yillar davomida minglab maxfiy xabarlarni o‘qishga muvaffaq bo‘lgan.

Xulosa

OneTimePad nazaiy jihatdan olib qaraganda, qiziqarli va shu bilan birga amalda qo‘llash juda murakkab va shubhali bo‘lishi mumkin. Vijener va OneTimePad o‘rtasidagi asosiy biz kutgan farq algoritmda emas, kalit tuzilishida.Vijener- bu deterministik usul va davr bilan takrorlanuvchi tizimdir. OneTimePad ehtimollik nazariyasiga asoslangan mutlaqo o‘zgacha tizim. Ammo agar kalit yaratishda haqiqiy sonlar o‘rniga random kutubxonalari ishlatilsa,algoritmni keying qadamlarini qaytadan hisoblash chiqish orqali buzish mumkin.

Foydalanilgan adabiyotlar:

1. Aulia Rahman Dalimunthe, Herman Mawengkang , Saib Suwilo , Ahmad Nazam ,“Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm”, 2019 J. Phys.: Conf. Ser. 1235 012030
2. Valentin Mulder • Alain Mermoud•Vincent Lenders•Bernhard Tellenbach, “Trends in Data Protection and Encryption Technologies”, https://doi.org/10.1007/978-3-031-33386-6
3. Shengyuan Wu, “One-time Pad Cipher Based on Out-Key Distribution”
4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949. – Vol. 28. – № 4. – P. 656–715.
5. Kahn D. The Codebreakers: The Comprehensive History of Communication from Ancient Times to the Internet. – Simon and Schuster, 1996. – 1181 p.
6. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th edition. – Pearson Education, 2017. – 768 p