Jizzax davlat Pedagogika Universiteti
TARIX FAKULTETI

HISTORY AND SOCIETY

ИСТОРИЯ И ОБЩЕСТВО
общественный электронный Журнал

№ 1

JOURNAL
2024

TARIX VA JAMIYAT ILMIY ELEKTRON JURNAL

2024-yil 1-son Ijtimoiy-gumanitar fanlar

Tarix, falsafa, huquq, sotsiologiya, tarix metodikasi

Bosh muharrir: Aqchayev F.Sh. JDPU, t.f.b.f.d. (PhD), dotsent.tarix fakulteti dekani

.

Bosh muharrir o‘rinbosari: Pardayev A.H. JDPU, tarix, t.f.n., dotsent

Mas’ul kotib: Karimova N.I JDPU, tarix,t.f.b.f.d (PhD)

TAHRIRIYAT A’ZOLARI:

1. Sagdullayev A.S. – tarix fanlari doktori, Akademik
2. Ahmedshina F.A. – tarix fanlari doktori, professor
3. Shodmonova S.B. – tarix fanlari doktori, professor
4. Ochilova B.M. – falsafa fanlari doktori, professor
5. Choriyev S. – falsafa fanlari doktori, professor
6. Tulenova G. J. – falsafa fanlari doktori, professor
7. Pardayev M.H. – tarix fanlari nomzodi, dotsent
8. G‘oyibov B.S. – tarix fanlari doktori (DSc), dotsent
9. Yarmatov R.B. – pedagogika fanlari doktori (DSc), professor
10. Saidqosimov A.I. – f.f.b. fan doktori (DSc), professor
11. Amanullayev A. – f.f.b. fan doktori (PhD), dotsent
12. Toshboyev F.E. – tarix fanlari bo‘yicha fan doktori (PhD), professor
13. Mirkomilov B. – tarix fanlari nomzodi, professor
14. Kobzeva.O.P. - tarix fanlari doktori, professor
15. G‘ofurov J.I – tarix fanlari bo‘yicha fan doktori (PhD), dotsent
16. Hoshimxonov M.X. – f.f.b. fan doktori (DSc), dotsent
17. Valiyev A.X. – katta o‘qituvchi
18. Majidov A.S. – katta o‘qituvchi

Dizayner va sahifalovchi: Karimova. N.I

MUNDARIJA

1. **MUNDARIJA** 3-4
2. **TARIX FANINI O'QITISHDA TARIXIY-BADIIY ADABIYOTLARDAN FOYDALANISHNING MAZMUNI VA MOHIYATI.** Ahror Pardayev Hasanovich. Zokirova Muxlisa. 5-9
3. **TURONNING BOHODIR VA DONO AYOLLARI.** Boltayev Abdurasul. Olim Mamarasulov. 9-14
4. **SOHIBQIRON AMIR TEMUR VA UNING HARBIY MAHORATI.** Boltayev Abdurasul. Abdullayev Abdulaziz 15-18
5. **MUSTAQILLIK YILLARIDA JIZZAX SHAHRINI ZAMONAVIY QIYOFAGA KELTIRISH.** Abdurasulova Dilbar To'raevna . Soatov Diyor 19-24
6. **FRIGIYA PODSHOLIGI.** Xamrayev G'ayrat G'aniyevich. Jumaqulova Diyora Ergashboy qizi. 25-29
7. **KUSHON DAVLATI TARIXI VA MADANIYATI XUSUSIDA.** O.Abdig'apparov. Nabiyeva Farmuda. 29-34
8. **MISR MADANIYATINING O'ZIGA XOS JIHATLARI.** O.Abdig'apparov. Naxalboyev Fozilbek. 34-38
9. **TA'LIMGA MILLIYLIK RUHI ASOSIDA RAQAMLI TEXNOLOGIYALARNI QO'LLASH SAMARADORLIGIGA OID.** J.O.Saidov. Shukurova Maftuna Alisher qizi. 38-43
10. **G'ARBIY YEVROPADA YANGI DAVR MADANIYATINING SHAKLLANISHI.** To'ychiyeva Dilnoza Ikromovna. Yo'ldoshev Bektemir Tursunboy o'g'li. 44-49
11. **ABDURAHMON JEVACHI — ERK VA OZODLIK KURASHCHISI.** B.Mirkomilov. Sh.Boymatov. 49-53
12. **РОЛЬ ЖЕНШИН В ЦЕНТРАЛЬНОЙ АЗИИ (КОНЕЦ XIX И НАЧАЛО XX ВЕКА).** Каримова Наргиза Икрамовна. Акрамова Навбахор. 53-58
13. **ПОЛИТИЧЕСКАЯ ЖИЗНЬ СРЕДНЕЙ АЗИИ В КОНЦЕ XIX - НАЧАЛЕ XX ВЕКА.** Каримова Наргиза Икрамовна. Бобокулова Севинч. 58-64
14. **DAVLATCHILIK TARIXIMIZDA SIYOSIY TRANSFORMATSIYANING NAMOYON BO'LISHI** Jamshid.Eshboyevich. Toshboyev. Abdug'aniyev Jahongir. 64-68
15. **TARIXIY ARXEOLOGIK MANBALAR VA UNING QADIM TARIXIMZDA TUTGAN O'RNI HAQIDA.** Furqat.Eshboyevich.Toshboev. R. Nosirova . 69-73
16. **LARSA SHAHRI XUSUSIDA BA'ZI MULOHAZALAR.** Tugalov Boburjon Baxodir o 'g'li**.** Karimov Boburjon Bobomurod o'g'li. 73-78
17. **ТОРГОВО-ЭКОНОМИЧЕСКАЯ И КУЛЬТУРНАЯ ЖИЗНЬ В СРЕДНЕЙ АЗИИ (В КОНЦЕ XIX - НАЧАЛО XX ВЕКА).** Каримова Наргиза Икрамовна, Машарипова Нодира. 78-84
18. **TEMURIYLAR DAVRIDA SIYOSIY JARAYONLAR.** Burxonov Lazizjon Salimjon o'g'li. Nurullayeva Farangiz Dilshod qizi. 85-89
19. **ТРАДИЦИИ И ОБЫЧАИ КАРАКАЛПАКОВ.** Каримова Наргиза Икрамовна Джумамуратова Инобат. 89-93
20. **YOZMA MANBALARDA KESH VA NAXSHAB TARIXINING YORITILISHI** Jo'raqulova Nurmohi Ne'matulla qizi. Bobur Karimov. 94-100
21. **KRIPTOGRAFIYA NIMA SABABDAN PAYDO BO'LDI YOXUD ILK SHIFRLASH NAMUNALARI.** Mirkomilov Baxtiyor.Axmedova Dildora Erkinjon qizi 100-105

KRIPTOGRAFIYA NIMA SABABDAN PAYDO BO‘LDI YOXUD ILK SHIFRLASH NAMUNALARI.

Professor. J.D.P.U. Mirkomilov Baxtiyor

J.D.P.U. Tarix fakulteti

3 kurs talabasi Axmedova Dildora Erkinjon qizi

Annotatsiya: Insoniyat bir-birini tushunib, so‘zlasha boshlaganiga ham bir necha ming yillar bo‘ldi. Qadimgi Misr, Mesopotamiya, Yunonlar sivilizatsiyada turli yozuv, belgilardan foydalanishgani hech kimga sir emas. Ularni har kim ham o‘qiy olmagan. Asrlar o‘tib sivilizatsiyani ichida saqlab kelayotgan bitiklarni o‘qish imkoni paydo bo‘ldi. Eyroglif, mixxat yozuvini o‘qish imkoni tug‘ildi. Shuncha qaramasdan, topilmalar orasidan yozuv bir qatorda tushunarsiz yoxud bolalar o‘yiniga o‘xshaydigan bir qancha hujjatlar ham topilgan. Ular shifrlangan edi. Bugungi kunda kodlar, yashirin belgilar bularning barchasi oddiy holga aylanishi tabiiy hol. Ba’zida bolalar o‘z do‘stlariga biror narsani eslatishda turli belgi yoki o‘zlarining so‘zlashuv usullaridan foydalanishadi. Uning ayrim turlari esa murakkab. Lekin ilk sivilizatsiyalar davrida ulardan nima maqsadda foydalanishgani juda g‘alati. Axir yozuv bir-birini tushinish uchun yetarli emasmi? Shifrlash- ma’lumotlarni xavfsizligini ta’minlash maqsadida ularni kodlash, shuningdek bir guruh odamlar tushuna oladigan ma’lumotlar hisoblanadi. Raqamli texnologiyalar paydo bo‘lishidan ancha oldin, xabarlarni begona ko‘zlardan himoya qilish usuli sifatida shifrlash paydo bo‘ldi. Uning ilk namunalaridan bezak berish, oshpazlar yoki hunarmandlar o‘z kasblaridagi boshqalarga bildirishni xohlamagan kasb sirlarini yozishda ham foydalanishgan.

Kalit so‘zlar: Shifrlash, maqbara, Scytale tayoqchasi, Hindiston, Yuliy Sezar, "Raqamli qal'a".

Abstract: It has been several thousand years since mankind began to understand and speak to each other. It's no secret that ancient Egypt, Mesopotamia, and the

Greeks used different writing and symbols in their civilization. Not everyone could read them. Centuries later, it became possible to read the inscriptions that keep the civilization inside. It became possible to read Euroglyph, cuneiform writing. Despite this, among the finds, several documents were found, the writing of which is incomprehensible or child's play. They were from encryption. Today, it is natural that codes, hidden symbols, all these things become commonplace. Sometimes children use different symbols or their own way of speaking to remind their friends. Some of its types are complex. But it is very strange for what purpose they were used in the period of early civilizations. Isn't writing enough to understand each other? Encryption is the encoding of data to ensure its security, as well as information that can be understood by a group of people. Long before the advent of digital technology, encryption emerged as a way to protect messages from prying eyes. Early examples of it were also used for decoration, and for writing down trade secrets that chefs or craftsmen did not want to share with others in their profession.

Keywords: Encryption, mausoleum, Scytale wand, India, Julius Caesar, "Digital Castle".

Аннотация: Прошло несколько тысяч лет с тех пор, как человечество начало понимать и разговаривать друг с другом. Ни для кого не секрет, что Древний Египет, Месопотамия и греки использовали в своей цивилизации разную письменность и символы. Не каждый мог их прочитать. Спустя столетия стало возможным прочитать надписи, хранящие внутри цивилизацию. Стало возможным читать евроглифы, клинопись. Несмотря на это, среди находок было обнаружено несколько документов, написание которых непонятно или является детской игрой. Они были зашифрованы. Сегодня вполне естественно, что коды, скрытые символы — все это становится обычным явлением. Иногда дети используют разные символы или свою собственную манеру речи, чтобы напомнить своим друзьям. Некоторые

из его типов сложны. Но очень странно, с какой целью их использовали в период ранних цивилизаций. Разве письма недостаточно, чтобы понять друг друга? Шифрование — это кодирование данных для обеспечения их безопасности, а также информации, которая может быть понята группой людей. Задолго до появления цифровых технологий шифрование возникло как способ защиты сообщений от посторонних глаз. Ранние примеры этого также использовались для украшения и записи коммерческих тайн, которыми повара или ремесленники не хотели делиться с другими представителями своей профессии.

Ключевые слова: Шифрование, мавзолей, палочка Скитейла, Индия, Юлий Цезарь, «Цифровой замок».

Qadimgi Misrda mil.avv. 1900 yillarda fir'avn Xnumxotep II maqbarasini oʻrganish jarayonida bir muncha murakkabroq boʻlgan yozuv namunasi topilgan. Maqbaradan topilgan bezakli eyrogliflarni tushunish qiyin boʻlgan. Undagi ma'lumotlarni tahlil qilish jarayoni ham koʻp vaqt talab etgan[1].

Mil.avv.1500 yillarda Mesopotamiyaning Dajla boʻyi hududlarida ham shifrlashdan foydalanilgani hududni oʻrganish jarayonida aniqlandi. Mesopotamiyada undan retseptlarni yashirishda foydalanilgan[1]. Retsept shunchaki taom tayyorlanish usullarini emas, balki hunarmandchilik buyumlarini yasash sir-sinoatlarini ham oʻz ichida jamlagan. Mesopotamiyada haykallar, turli xoʻjalik mahsulotlari yasash uslublari boshqa joylarda uchramaydi. Buni oʻz kasbining ustalari qila olgan holos. Ammo oradan koʻp vaqt oʻtmay ularni shifrlash mohiyatini boshqalar tushunib qoladi. Bu oddiy boʻlgani uchun ham boshqalar belgilarni ma'nosini anglashga qiynalmagan. Keyinchalik bu keng tarqala boshlagan.

Shifrlardan kasb nuqtai nazaridan tashqari kundalik hayotda ham foydalanilgan boʻlishi mumkin. Xususan, Hindistonda erkak va ayol bir-biri bilan kodlangan xabarlar orqali soʻzlashgan jarayonlari tadqiqot jarayonlari topilgan bitiklardan

o‘rganilgan[1]. Bunday holatlar oiladagi boshqalar bilishi kerak bo‘lmagan sir yoxud inson shaxsiyatiga tegishli bo‘lgan ma’lumotlarni bir biriga aytishda yashirin so‘zlashuv usulini o‘ylab topishgan. Bu orqali o‘zlari bilmagan xolda shifrlashning yangi bosqichini boshlab berdi desak yanglishmagan bo‘lamiz. Bunday xabarlashish bugungi kunda ham oila a'zolari orasida mavjud.

Oradan vaqt o‘tib, kodlashni bir muncha murakkab shakllari ham shakllanadi. Shifrlashdan harbiy maqsadlarda Yunoniston hududida foydalanilgan. Buning uchun yunonlar qalin tayoq yoxud maxsus metall va qog‘ozdan foydalanishdi. Qozog‘ni qalin tayoqqa o‘rab, ma’lumot tayoq uzunligi bo‘yicha yozilgan. So‘ng qog‘oz tayoqdan bo‘shatilib, yuborilishi kerak bo‘lgan insonga eltib berilgan. Bunday tayoq uni olgan insonda ham bo‘lgan va u qog‘ozni tayoqqa o‘rab, unda nima yozilganini bilib olgan. Bu usul tarixda Scytale deb atalgan[1]. Vaqt o‘tib, u yanada takomillashib borgan.

Yuqoridagi rasmda Scytalening qadimgi va zamonaviy ko‘rinishi hisoblanadi. Zamon rivojlanib, uning yangi turlari ham ixtiro qilingan. Scytale ma’lum bir diametrli novda atrofida pergament chizig‘ini o‘rash va ana shu pergament uzunligi bo‘ylab xabar yozishni o‘z ichiga oladi. Rasmdagi uskunalar ko‘rinishidan murakkabga o‘xshaydi. Ammo u o‘z davri uchun muhim ma’lumotlarni yetkazishda asosiy qurol hisoblangan. U dushman qo‘lida tushgan taqdirda ham uni ya'ni harflarni joylashtirish texnikasini bilmaganlar uchun bu oddiy bir matoh bo‘lgan xolos.

Insoniyat rivojlanib, uni yangi bilim egallashga bo‘lgan qiziqishi ortib bordi. Scytaledan ham bir muncha murakkabroq shaklini Rimlik Yuliy Sezar tomonidan yaratilgan. Matnlarni kodlash Rim imperatori Yuliy Sezar o‘zining "Galiya

yurishlari xotiralarim" nomli kitobida keltirilib o‘tilgan[1]. Bilamizki, Yuliy Sezar davrida Rim hududini kengaytirish, mutlaq hokimiyatni o‘rnatishga harakat boshlagan edi. Imperatorning xat eltuvchilariga hujum avj olib, uning xabarlari dushmanlarining qo‘liga tusha boshlagan va u nimani rejalashtirgani, keyingi yurish rejalari o‘g‘irlanadi. U tuzgan rejalarini dushmanlardan himoyalash yoxud ularning qo‘liga tushgan taqdirda ham tushuna olmaydigan qilib yozishni o‘ylab topdi. Sezarning o‘zi va sarkardalar biladigan maxfiy muloqotni - shifrlashni o‘ylab topdi va ularga ham buni o‘rgatdi. General Sezar kodlashda alifbodagi harflar o‘rnidan ustalik bilan foydalandi. Alifbodagi bir harfni ma’lum qator va tartib raqamidagi harf bilan o‘rin almashtirgan holda xabarni kodlaydi. Misol uchun, birinchi harfning o‘rniga alifboda undan keyingi 4-harfni yozgan. Harflar ketma-ketligini oldinga yoki orqaga ma’lum tartibda siljitish matndagi xabarni yashirishga xizmat qilgan[1].

Yuqorida ko‘rilgan qadimgi dunyo tarixidan misollar. Kimdir undan kasb sirlarini saqlashda foydalansa, yana kimdir harbiy maqsadda foydalangan. Shuning faol turmush tarzida ham uning o‘rni kattaligini bilib oldik. Undan faqat ezgu maqsadlarda foydalanilgan desak, biroz xatoga yul quygan bo‘lamiz. Ayrim hollarda shifrovkalar xalokat sari yetaklashi mumkin. Buni oldini olish uchun har qanday kodlari yecha oladigan kriptograflar faol harakat qilmoqda. O‘tgan asrning 80-90-yillarida Enigma nomli maxsus qurilma yaratildi. Uning xotirasiga barcha kod, shiftlar va ularning yechilish usul, uslublari joylandi. Bu orqali terrorchi yoxud yovuz maqsadi bo‘lgan insonlarni rejasi fosh etilgan. Den Braunning "Raqamli qal'a" nomli kitobida shifr, kod, maxfiy xabar, razvedka aloqalari to‘g‘risida atroflicha keltirilib o‘tilgan[1].

Xulosa shundan iboratki, kriptografiya fani yillar mobaynida turli xil xolatda sodir bo‘lgan voqealarni o‘rganishda juda katta ahamiyatga ega ekanligini ko‘rib turibmiz. Hozirgi globallashuv jarayonida dunyoning turli mamlakatlarida faoliyat ko‘rsatadigan xalqlarning bevosita o‘ziga tegishli bo‘lgan (sirlarini) davlat ahamiyatiga molik, xalqlarning turmushiga tegishli holatlarni saqlashda biz

o‘rganayotganimiz kriptografiya san’ati, sirlarini shifrlash sohasi katta o‘rin egallaydi.

Fotdalangan adabiyotlar ro‘yxati:

1. Firdavs Umed o‘g‘li Jo‘rayev, Raxila Xasanova “Kriptrografiya sohasining kelib chiqishi” maqolasi October 20,2023

2. Rebekka Beylz “Kriptografiya tarixi” maqola, August 1, 2023

3. Sasha Blakeley, Louay Chebib “History of Encryption, Invertion & Types” 11/21/2023

4. ThanoDev “The Fascinating History of Encyption: From Ancient Greeks to modern Cybersecurity” sep 22, 2023

5. Thomas “The history and future of encryption” November 3, 2023.

6. Ден Браун “Рақамли қальа” 2-Нашр Тошкент 2019.

7. https://www.encryptmylaptop.com/history-of-encryption

8. https://cspi.uz/