

УДК: 003.26:004.056.55

DOI: 10.65599/III6501

ТАҲИЯИ КАЛИДИ БАДАЛСОЗӢ БО ТАРЗИ СТАХОСТИКӢ АЗ ИСТИФОДАИ ҲИЧО ВА МАССИВҲОИ ЯКЧЕНАКА ДАР БАДАЛСОЗИИ ОБЪЕКТҲОИ МАТНӢ

М.Ҳ. Гафуров, Д.А. Анварзода

Донишгоҳи техникии Тоҷикистон ба номи академик М.С. Осимӣ, ш. Душанбе, Ҷумҳурии Тоҷикистон

Дар пажӯҳиши мазкур равиши нави ташаққули калидҳои бадалсозӣ барои маълумоти матнӣ бо истифода аз усули стохастикӣ пешниҳод шудааст. Назарияи асосӣ бар он асос ёфтааст, ки воҳидҳои гуногуни забонӣ (лингвистикӣ) — ба монанди решаи калимаҳо, пешоянду пасояндҳо, аффиксҳо, инчунин аломатҳои китобатию махсус — бо массивҳои якченака алоқаманд карда мешаванд. Бо ин роҳ, раванди ҷиҳатсозии матн бевосита дар заминаи хусусиятҳои лингвистикӣ ва алифбои худӣ ҳамон забон амалӣ мегардад. Ҳадафи асосии татбиқи ин алгоритм баланд бардоштани сатҳи амнияти иттилоотӣ ва ҳифзи додаҳо аз даҳлати бечозат ё ҳамлаҳои киберӣ (ҳакерҳо, қулфшиканҳо) мебошад. Ҳамзамон, дар мақола дараҷаи устувории чунин калидҳо ва хатари эҳтимолии шикастани онҳо ба таври муфассал таҳлил гардидааст. Бояд қайд намуд, ки усули коркардшуда хусусияти универсалӣ дошта, онро метавон дар матнҳои забонҳои дигар низ беамониат истифода бурд.

Калидвожаҳо: объект, бадалсозӣ, бадалкунӣ, аксбадалкунӣ, реша, аломатҳои имлоию махсус, алифбои хусусӣ, калид, вариант, устуворӣ, киберҷиноят.

РАЗРАБОТКА СТОХАСТИЧЕСКОГО КЛЮЧА ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ СЛОГОВ И ОДНОМЕРНЫХ МАССИВОВ ПРИ ШИФРОВАНИИ ТЕКСТОВЫХ ОБЪЕКТОВ

М.Х. Гафуров, Д.А. Анварзода

Таджикский технический университет имени академика М.С. Осими, г. Душанбе, Республика Таджикистан

В данном исследовании предложен новый подход к формированию ключей шифрования текстовой информации с использованием стохастического метода. Основная идея заключается в том, что различные языковые единицы - такие как слоги, а также орфографические и специальные символы - сопоставляются с одномерными массивами. Таким образом, процесс шифрования текста осуществляется непосредственно на основе лингвистических особенностей и собственного алфавита соответствующего языка. Основной целью реализации данного алгоритма является повышение уровня информационной безопасности и защита данных от несанкционированного доступа или кибератак (хакеров). В работе также подробно проанализированы степень устойчивости таких ключей и вероятность их возможного взлома. Следует отметить, что разработанный метод обладает универсальным характером и может быть эффективно применён для обработки текстов на различных языках.

Ключевые слова: объект, шифрования, зашифрования, расшифрования, слоги, орфографические и специальные символы, частный алфавит, ключ, вариант, устойчивость, киберпреступление.

DEVELOPMENT OF A STOCHASTIC ENCRYPTION KEY USING SYLLABLES AND ONE-DIMENSIONAL ARRAYS FOR TEXT OBJECT ENCRYPTION

M.Kh. Gafurov, D.A. Anvarzoda

Tajik Technical University named after academician M.S. Osimi, Dushanbe, Republic of Tajikistan

This study proposes a novel approach to generating encryption keys for textual information using a stochastic method. The core concept involves mapping various linguistic units—such as syllables, as well as orthographic and special characters - to one-dimensional arrays. Consequently, the text encryption process is performed directly based on the linguistic characteristics and the specific alphabet of the target language. The primary objective of implementing this algorithm is to enhance information security and protect data from unauthorized access or cyberattacks. The paper also provides a detailed analysis of the robustness of these keys and the probability of their potential compromise. It should be noted that the developed method is universal in nature and can be effectively applied to the processing of texts in various languages.

Keywords: object, encryption, enciphering, decryption, syllables, orthographic and special characters, specific alphabet, key, variant, robustness, cybercrime.

Муқаддима (Introduction)

Дар аксари равишҳои анъанавии бадалсозии маълумот, ҳамчун асос алифбои стандартӣ забон баромад намуда, ба ҳар як аломати матнӣ кушода рақами мушаххас бахшида мешавад. Чунин тарзи кор - аз шифрҳои таърихи Сезару Полибий сар карда, то баъзе алгоритмҳои муосир - ба таври васеъ маъмул аст ва маъмулан онро бадалсозии униграммавӣ меноманд. Дар ин ҳолат, раванди ҷиҳатсозии матн тибқи қоидаҳои муайян ва дар заминаи калиди махфӣ сурат мегирад, ки ин раванд дар як қатор қорҳои илмӣ [1-9] ба таври васеъ баррасӣ ёфтааст.

Бо вучуди ин, дар замони муосир рушди босуръати технологияҳои ҳисоббарор, бахусус пайдоиши суперкомпютерҳо ва мошинҳои квантӣ, амнияти чунин алгоритмҳои зерин хатар меғузорад. Иқтидори баланди ҳисоббарории имрӯза ба криптоаналитикҳо ва киберҷинояткорон имкон медиҳад, ки тавассути таҳлили басомади (зуддии) пайдоиши символҳо, матнӣ бадалшударо ба осонӣ таҳлил намуда, ба ҳолати аввалааш (кушода) баргардонанд.

Барои рафъи ин осебпазирӣ, дар мақолаҳои [10-14] равишҳои наву муосир пешниҳод шудаанд. Дар онҳо роҳҳои ташаққули алифбои хусусии бадалсозӣ, таҳияи калидҳои нави муҳофизатӣ ва инчунин татбиқи калидҳои ёрирасоне, ки сохтори аслии объекти матнро ҳангоми аксбадалкунӣ ҳифз мекунанд, мавриди омӯзиш қарор гирифтаанд.

Алгоритми ҳалли масъала (Algorithm for solving the problem)

Дар заминаи равишҳои дар тадқиқоти [10-14] пешниҳодшуда, қараёни пӯшидасозии матнро бо истифода аз усули стохастикӣ таҳлил мекунем. Дар ин ҳолат калиди криптографӣ мустақиман аз хусусиятҳои лингвистии ҳуди матн (ҳиҷо, аломатҳои китобатӣ) ва массивҳои якченака, инчунин бо ҷалби калиди ёрирасон ташаккул меёбад.

Пайдарпайии амалисозии ин алгоритм чунин аст:

1. **Омодасозии матн:** Дар оғоз объекти матнии кушода (минбаъд — объекти $\mathcal{L}$) интиҳоб ва ё таҳия карда мешавад.

2. **Тақсимои лингвистӣ:** Объекти мазкур ба ҷузъҳои хурдтарини забонӣ — ҳиҷо ва дигар аломатҳои имлоиву махсус таҷзия мегардад.

3. **Эҷоди калиди ёрирасон (K_6):** Барои нигоҳ доштани сохтори аслии матн (аз ҷумла фосилаҳо ва сархатҳо) ҳангоми бадалсозӣ ва аксбадалкунӣ, калиди махсуси ёрирасон сохта мешавад. Унсурҳои ивазкунандаи ин калид аз пойгоҳи стандартҳои ASCII ё UNICODE интиҳоб мешаванд.

4. **Татбиқи K_6 :** Бо ёрии калиди ёрирасони таҳияшуда, объекти кушодаи $\mathcal{L}$ ба шакли мобайнии $\mathcal{L}_1$ табдил дода мешавад.

5. **Ташаккули алифбои хусусӣ:** Аз тамоми ҷузъҳои забонии дар боло зикршуда (ки аллакай тавассути калиди K_6 қисман иваз шудаанд), алифбои беназири бадалсозии A_x барои матни додашуда таҳия карда мешавад.

6. **Муайянкунии массив:** Вобаста ба миқдори унсурҳои, ки дар алифбои A_x ҷамъ омадаанд, ба ҳамон миқдор унсур аз массиви якченака интиҳоб карда мешавад.

7. **Сохтани калиди асосӣ (K_a):** Бо истифода аз қонуниятҳои стохастикӣ, ҳар як унсури алифбои A_x ба як унсури массиви якченака пайваست карда шуда, калиди асосӣ K_a , ки он махфӣ мебошад таҳия карда мешавад.

8. **Бадалсозии ниҳой:** Дар ин қадам, тавассути калиди асосии K_a , объекти мобайнии $\mathcal{L}_1$ пурра бадалсозӣ гардида, матни ниҳойи пӯшидаи $\mathcal{L}_2$ ҳосил мешавад.

9. **Раванди аксбадалкунӣ:** Барои кушодани объекти бадалшудаи $\mathcal{L}_2$ амалҳо бо тартиби баръакс иҷро мешаванд: нахуст тавассути калиди K_a объекти $\mathcal{L}_2$ ба ҳолати $\mathcal{L}_1$ баргардонида мешавад ва сипас, бо истифода аз калиди ёрирасони K_6 сохтори матн барқарор шуда, объекти аслии $\mathcal{L}$ ба даст меояд.

Ҳалли масъала дар мисолҳо (Problem solving through examples)

Барои амалӣ намудани алгоритми пешниҳодшуда, матни аслии $\mathcal{L}$ тавассути калиди таҳияшудаи бадалсозӣ пӯшида гардонида мешавад. Ин калид бевосита дар асоси алифбои хусусӣ ва массиви якченака сохта шудааст. Фарз мекунем, ки объекти $\mathcal{L}$ рубоии зерини Умари Хайём мебошад:

$$\mathcal{L} = \left\{ \begin{array}{l} \text{Хайём, агар зи бода мастӣ, хуш бош!} \\ \text{Гар бо санаме даме нишастӣ, хуш бош!} \\ \text{Поёни ҳама кори ҷаҳон нестӣ аст,} \\ \text{Пиндор, ки нестӣ, чу ҳастӣ, хуш бош!} \end{array} \right\} \quad (1)$$

Дар асоси марҳилаи дуҷуми алгоритми пешниҳодшуда, объекти ибтидоии $\mathcal{L}$ ба ҷузъҳои таркибияш таҷзия карда мешавад. Ин ҷузъҳо ҳиҷо, инчунин аломатҳои китобатӣ махсус ва дигар унсурҳои ҷумларо дар бар мегиранд. Дар натиҷаи ин амал, объект шакли нави $\mathcal{L}_1$ -ро пайдо мекунад, ки намуди зерин дорад:

$$\mathcal{L}_1 = \left\{ \begin{array}{l} \text{Хай — ём, а — гар зи бо — да мас — тӣ, хуш бош!} \\ \text{Гар бо са — на — ме да — ме ни — шас — тӣ, хуш бош!} \\ \text{По — ё — ни ҳа — ма ко — ри ҷа — ҳон нес — тӣ аст,} \\ \text{Пин — дор, ки нес — тӣ, чу ҳас — тӣ, хуш бош!} \end{array} \right\} \quad (2)$$

Бо дарназардошти аломатҳои мавҷудаи объект, калиди ёрирасон таҳия карда мешавад. Рамзҳои ҷойгузини ин калид аз ҷадвалҳои стандартҳои ASCII ё UNICODE интиҳоб гардида, бояд ҳатман аз аломатҳои ҳуди объекти $\mathcal{L}$ фарқ кунанд. Истифодаи аломати сархат (абзатс) дар калиди ёрирасон барои он зарур аст, ки сохтори аслии объект ҳангоми раванди табдилдиҳии баръакс (аксбадалсозӣ) қомилан нигоҳ дошта шавад. Фарз мекунем, ки ин калид намуди зерин дорад:

$$K_{\bar{e}} = \{ \rightarrow s, ! \rightarrow v, \cup \rightarrow h, \lrcorner \rightarrow t \} \quad (3)$$

Бо истифода аз калиди таҳишудаи ёрирасон $K_{\bar{e}}$ объекти $\mathcal{L}$ -ро ба шакли пайдарпаии унсурҳо меорем, ки он $\mathcal{L}_2$ чунин намудро мегарад:

$$\mathcal{L}_2 = \left\{ \begin{array}{l} \text{Хай} - \text{ём } s \text{ } h \text{ } a - \text{гар } h \text{ } \text{зи } h \text{ } \text{бо} - \text{да } h \text{ } \text{мас} - \text{тӣ } s \text{ } h \text{ } \text{хуш } h \text{ } \text{бош } v \text{ } t \\ \text{Гар } h \text{ } \text{бо } h \text{ } \text{са} - \text{на} - \text{ме } h \text{ } \text{да} - \text{ме } h \text{ } \text{ни} - \text{шас} - \text{тӣ } s \text{ } h \text{ } \text{хуш } h \text{ } \text{бош} \\ v \text{ } t \text{ } \text{По} - \text{ё} - \text{ни } h \text{ } \text{ҳа} - \text{ма } h \text{ } \text{ко} - \text{ри } h \text{ } \text{ча} - \text{ҳон } h \text{ } \text{нес} - \text{тӣ } h \text{ } \text{аст } s \\ t \text{ } \text{Пин} - \text{дор } s \text{ } h \text{ } \text{ки } h \text{ } \text{нес} - \text{тӣ } s \text{ } h \text{ } \text{чу } h \text{ } \text{ҳас} - \text{тӣ } s \text{ } h \text{ } \text{хуш } h \text{ } \text{бош } v \end{array} \right\} \quad (4)$$

Дар марҳилаи навбатӣ, дар заминаи унсурҳои дохили объекти $\mathcal{L}_2$, мо алифбои хусусии бадалсозиро барои матни мазкур ташаккул медиҳем. Сохтори ин алифбо намуди зеринро касб мекунад:

$$A_x = \{ \text{Хай, ём, а, гар, зи, бо, да, мас, тӣ, хуш, бош, Гар, са, на, ме, ни, шас, По, ё, ҳа, ма, ко, ри, ча, ҳон, нес, аст, Пин, дор, ки, чу, ҳас, } h, s, v, t \} \quad (5)$$

Аз унсурҳои дар алифбои хусусии бадалсозии объекти додашуда (5) истифода карда, яке аз варианти калиди бадалсозии асоси K_a -ро таҳия мекунем, ки дар он ҳар як унсур бо тарзи стахостикӣ ба унсурҳои массиви якченака иваз карда мешавад, ки дар ҷадвали зерин оварда шудааст.

Ҷадвали 1 – Калиди асосии бадалсозии K_a

Table 1 – The primary key for K_a substitution

шас	Пин	ҳа	ё	на	бош	ме	Хай	ко	ҳас	s	аст
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}

ём	v	ни	бо	ма	Гар	хуш	гар	чу	ки	тӣ	ри
a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}

а	да	h	По	ча	ҳон	t	нес	са	мас	дор	зи
a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	a_{36}

Бо татбиқи варианти таҳияшудаи калиди асосии K_a , объекти кушода, ки дар шакли (4) пешниҳод гардидааст, бадалсозӣ карда мешавад. Дар натиҷаи ин раванд, объекти нави бадалшудаи $\mathcal{L}_3$ ҳосил мегардад, ки он намуди зеринро дорад:

$$\mathcal{L}_3 = \left\{ \begin{array}{l} a_8 a_{13} a_{11} a_{27} a_{25} a_{20} a_{27} a_{36} a_{27} a_{16} a_{26} a_{27} a_{34} a_{23} a_{11} a_{27} \\ a_{19} a_{27} a_{6} a_{14} a_{31} a_{18} a_{27} a_{16} a_{27} a_{27} a_{5} a_{7} a_{27} a_{26} a_{7} a_{27} a_{15} \\ a_1 a_{23} a_{11} a_{27} a_{19} a_{27} a_6 a_{14} a_{31} a_{28} a_4 a_{15} a_{27} a_3 a_{17} a_{27} \\ a_9 a_{24} a_{27} a_{29} a_{30} a_{27} a_{32} a_{23} a_{27} a_{12} a_{11} a_{31} a_2 a_{35} a_{11} a_{27} \\ a_{22} a_{27} a_{32} a_{23} a_{11} a_{27} a_{21} a_{27} a_{10} a_{23} a_{11} a_{27} a_{19} a_{27} a_6 a_{14} \end{array} \right\} \quad (6)$$

Аз объекти бадалшудаи $\mathcal{L}_3$ бармеояд, ки он аз пайдарпаии массиви якченака иборат буда, ба қулфшиканҳо (хакерон, киберчинояткорон ё шахсони алоҳидаи ҳавасманд) маънои муайянеро намедиҳад. Онҳо танҳо дар ҳолати дастрас кардани варианти калиди асосӣ ва ёрирасон метавонанд онро ба объекти аввалаи кушода баргардонид ба маънои он шинос гарданд.

Дар ҳолати бо ягон роҳ пайдо кардани баъзе аз маълумотҳои усули мазкур, ки миқдори вариантҳои калиди асосӣ аз рӯи формулаи зерин $U = N_1!$, ки дар инҷо $N_1 = 36$ миқдори умумии унсурҳо дар алифбои хусусии бадалсозӣ буда $U \approx 3.72 \cdot 10^{41}$ мебошад, эҳтимолияти муайян кардани калиди асосӣ $U_1 = 1/N_1! \approx 0.27 \cdot 10^{-41}$ мешавад ва ҳангоми бадалсозии объектҳои матнии ҳаҷман калон миқдори унсурҳои алифбои хусусӣ мутаносибан меафзояд. Дар натиҷа миқдори вариантҳои калиди асосии бадалсозӣ боло меравад ва муайянсозии он низ хеле душвор (ҳисобкунии он ба беохири майл мекунад) мегардад.

Дар усули мазкур истифодаи ҷойивазкунии унсурҳои объекти бадалшуда барои муайнсозии объекти матнии кушода татбиқнашаванда мебошад, чунки он аз пайдарпаии массиви якченакаи иборат буда, танҳо дар ҳолати муайянсозии варианти калиди асосии таҳияшудаи бадалсозии дар ҷадвал овардашуда ва калиди ёрирасон имконияти он ҷой дорад. Агар ҳолати ҷойивазкуниро истифода кунем, ҳамаи унсурҳои объекти кушодаи дигаргуншудаи дар (6) оварда, ки миқдори унсурҳояш ба 81 баробар мебошад ва тасодуфан бо ягон роҳ ҳар як массиви он муайян шуда бошад, пас $81! \approx 5.8 \cdot 10^{120}$ ҷойивазкунии ҷой дорад ва он аз тамоми атомҳои (заррачаҳои хурд) дар галактикаи мо буда якчанд маротиба зиёд мебошад ва онро (ҳисобкуниҳоро) на танҳо компютерҳои замонавӣ, ҳатто компютерҳои дар оянда сохташаванда (аз ҷумла квантӣ) низ қудрати муайян кардани надоранд. Яъне усули ҷойивазкунии дағал "брутфорс" - ҷустуҷӯи ҳамаҷониба (ё усули «нерӯи дағал», аз англ. brute force) - ин усули муайян ва ҳал кардани масъалаҳои риёзӣ ва криптографӣ мебошад, ки тавассути сараввал дида баромадан ва санҷидани тамоми вариантҳои имконпазир сурат мегирад, ғайри қобили қабул аст.

Аксбадалкунии объекти бадалшудаи $\mathcal{L}_3$ ва овардани он ба объекти кушодаи $\mathcal{L}$ тибқи талаботи банди 9-и алгоритми ҳалли масъала амалӣ карда мешавад.

Хулоса (Conclusions)

Бартариҳо ва хусусиятҳои асосии усули таҳияшударо метавон ба тариқи зайл ҷамъбаст намуд:

1. Хусусияти универсалӣ: Равиши пешниҳодшуда бо ягон забони мушаххас маҳдуд намегардад. Онро метавон бемамоният барои ҳифзи маълумоти матнӣ дар забони ихтиёрӣ татбиқ намуд.

2. Муҳофизати базавӣ (Сатҳи якум): Бархилофи алгоритмҳои анъанавӣ, ки асосан ба ивазкунии рамзҳои символҳои алоҳида таъяс мекунанд, дар ин усул воҳидҳои лингвистӣ ҳамчун унсурҳои асосии бадалсозӣ баромад мекунанд. Ин муносибати нав сади аввалини мустаҳкамро дар баробари даҳолати беиҷозат ба вуҷуд меорад.

3. Ҳимояи иловагӣ ва ҳифзи сохтор (Сатҳи дуюм): Ҷорӣ намудани калиди ёрирасон на танҳо қарорати медиҳад, ки сохти аслии ҳуҷҷат ҳангоми аксбадалкунии пурра барқарор шавад, балки он ҳамчун қабати дуюми амниятӣ амал карда, сатҳи муҳофизати маълумотро баланд мебардорад.

4. Муқовимат муқобили криптоатақил: Яке аз дастовардҳои муҳимтарини ин алгоритм он аст, ки вай имконияти татбиқи таҳлили басомадии униграммавиро (яъне ошкорсозӣ тавассути ҳисоби такроршавии символҳо) қомилан бекор месозад. Маҳз ҳамин намуди таҳлил силоҳи маъмултарини қулфшиканон ва ҳакерон ба шумор меравад, аммо усули пешниҳодшуда ин осебпазирро аз байн мебарад.

Муқарриз: Мирзоев С.Х. – д.и.т., профессори кафедраи информатикаи Донишгоҳи миллии Тоҷикистон.

Адабиёт

1. Виженер Б. Трактат о шифрах / пер. с фр. — М.: Наука, 1996.
2. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 333–402.
3. Басалова Г.В. Основы криптографии. Тула: Изд-во Тульского государственного университета, 2009.
4. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. М.: Бином, 2007.
5. Левин М. Криптография без секретов: Руководство пользователя. М.: Новый издательский дом, 2005.
6. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
7. Шнайер Б., Фергюсон Н. Практическая криптография. М.: Диалектика, 2005.
8. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
9. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
10. Гафуров, М. Х. Об одном способе шифрования объекта с использованием элементов языка / М. Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2023. № 2 (62). С. 22–29. EDN: GABKCE.
11. Гафуров, М. Х. Шифрование элементов текста матричным и оператор - матричным методами / М. Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2024. № 4 (68). С. 30–35. EDN: NKNVOJ.
12. Гафуров, М. Х. Такмили усули Виженер дар бадалсозии объектҳои матнӣ / М. Х. Гафуров // Паёми политехникӣ. Баҳши: Интеллект, Инноватсия, инвеститсия. 2025. No. 2(70). P. 67–71. — EDN ZWPXCB.
13. Гафуров, М. Х. Об одном способе шифрования текстовых объектов с использованием нумерации его элементов / М. Х. Гафуров // Доклады Национальной академии наук Таджикистана. 2025. Т. 68, № 7. С. 655–664. — EDN PUIVMF.
14. Гафуров, М. Х. Шифрования текстовых элементов с использованием метода Виженера / М. Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2026. № 1(73). — С. 99–110. — DOI 10.65599/III531. — EDN VSNQBE.

Reference

1. Vigenère, B.. Traicté des Chiffres ou Secrètes Manières d'Ecrire [Treatise on Ciphers]. (Transl. from French). Moscow: Nauka, 1996.
2. Shannon, C. E. Communication Theory of Secrecy Systems. In Works on Information Theory and Cybernetics (pp. 333–402). Moscow: IL, 1963.
3. Basalova, G. V. Fundamentals of Cryptography. Tula: Tula State University Publishing House, 2009.
4. Burnett, S., & Paine, S. RSA Security's Official Guide to Cryptography. Moscow: Binom, 2007.
5. Levin, M. Cryptography Without Secrets: A User's Guide. Moscow: Novy Izdatelsky Dom, 2005.
6. Mao, W. Modern Cryptography: Theory and Practice. Moscow: Williams, 2005.
7. Schneier, B., & Ferguson, N. Practical Cryptography. Moscow: Dialektika, 2005.
8. Singh, S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Moscow: Ast, Astrel, 2006.
9. Bauer, F. L. Decrypted Secrets: Methods and Maxims of Cryptology. Moscow: Mir, 2007.
10. Gafurov, M. Kh. On a method of object encryption using language elements. Polytechnical Bulletin. Series: Intelligence. Innovations. Investments. 2023. (2), 22-29. EDN: GABKCE.
11. Gafurov, M. Kh. Encryption of text elements by matrix and operator-matrix methods. Polytechnical Bulletin. Series: Intelligence. Innovations. Investments. 2024. (4), 30-35. EDN: NKNVOJ.
12. Gafurov, M. Kh. Improvement of the Vigenère method in the substitution of text objects. Polytechnical Bulletin. Section: Intelligence, Innovation, Investment. 2025. (2), 67-71. EDN: ZWPXCB.
13. Gafurov, M. Kh. On a method of encrypting text objects using the numbering of its elements. Reports of the National Academy of Sciences of Tajikistan. 2025. 68(7), 655-664. EDN: PUIVMF.
14. Gafurov, M. Kh. Encryption of text elements using the Vigenère method. Polytechnical Bulletin. Series: Intelligence. Innovations. Investments. 2026. (1), 99-110. DOI: 10.65599/III3531. EDN: VSNQBE.

Маълумот оид ба муаллифон:

Гафуров Миршафи Ҳамитович, номзади илмҳои техникӣ, дотсент, дотсенти кафедраи амнияти киберии системаҳои иттилоотии факултети технологияҳои рақамӣ, системаҳо ва ҳифзи иттилооти донишгоҳи техникии Тоҷикистон ба номи академик М.С. Осими. ORCID: <https://orcid.org/0000-0001-8173-7650>, E-mail: mirugaf56@gmail.com

Анварзода Далер Анвар, номзади илмҳои техникӣ, и.в. дотсенти кафедраи телекоммуникатсия ва технологияҳои шабакавии факултети технологияҳои рақамӣ, системаҳо ва ҳифзи иттилооти донишгоҳи техникии Тоҷикистон ба номи академик М.С. Осими. ORCID: <https://orcid.org/0000-0003-1102-8140>, E-mail: daler@ttu.tj

Сведения об авторах:

Гафуров Миршафи Ҳамитович, кандидат технических наук, доцент, доцент кафедры кибербезопасности информационных систем факультета цифровых технологий, систем и защиты информации Таджикского технического университета имени академика М. С. Осими. ORCID: <https://orcid.org/0000-0001-8173-7650>, E-mail: mirugaf56@gmail.com

Анварзода Далер Анвар, кандидат технических наук, и.о. доцента кафедры телекоммуникаций и сетевых технологий факультета цифровых технологий, систем и защиты информации Таджикского технического университета имени академика М. С. Осими. ORCID: <https://orcid.org/0000-0003-1102-8140>, E-mail: daler@ttu.tj

Information about the authors:

Gafurov Mirshafi Hamitovich, PhD in Technical Sciences, Associate Professor, Associate Professor at the Department of Cybersecurity of Information Systems, Faculty of Digital Technologies, Systems and Information Security, Tajik Technical University named after Academician M.S. Osimi. ORCID: <https://orcid.org/0000-0001-8173-7650>, E-mail: mirugaf56@gmail.com

Anvarzoda Daler Anvar, PhD in Technical Sciences, Acting Associate Professor at the Department of Telecommunications and Network Technologies, Faculty of Digital Technologies, Systems and Information Security, Tajik Technical University named after Academician M.S. Osimi. ORCID: <https://orcid.org/0000-0003-1102-8140>, E-mail: daler@ttu.tj