Торайғыров университетінің
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

ТОРАЙҒЫРОВ УНИВЕРСИТЕТІНІҢ ХАБАРШЫСЫ

ПЕДАГОГИКАЛЫҚ СЕРИЯСЫ

1997 ЖЫЛДАН БАСТАП ШЫҒАДЫ

TORAIGHYROV UNIVERSITY

ВЕСТНИК ТОРАЙГЫРОВ УНИВЕРСИТЕТА

ПЕДАГОГИЧЕСКАЯ СЕРИЯ

ИЗДАЕТСЯ С 1997 ГОДА

ISSN 2710-2661

№ 2 (2023)

ПАВЛОДАР

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

Педагогическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ KZ03VPY00029269
выдано
Министерством информации и коммуникаций
Республики Казахстан

Тематическая направленность
публикация материалов в области педагогики,
психологии и методики преподавания

Подписной индекс – 76137

https://doi.org/10.48081/LQYE2220

МРНТИ 81.93.29

https://doi.org/10.48081/JUKB4198

М. Серік[1], Д. Ш. Тлеумагамбетова[2]
[1,2]Л. Н. Гумилев атындағы Еуразия Ұлттық университеті,
Қазақстан Республикасы, Астана қ.
e-mail: *serik_meruerts@mail.ru

«АҚПАРАТТЫҚ ҚАУІПСІЗДІК» КУРСЫ БОЙЫНША КЕЙБІР СҰРАҚТАРДЫ ОҚЫТУҒА АРНАЛҒАН ӘДІСТЕМЕЛІК НҰСҚАУЛЫҚТАР

Бүгінгі таңда ақпараттық-коммуникациялық технологиялар мен Интернеттің қарқынды дамуына байланысты, қауіпсіздік шараларының жетілдірілуіне қарамастан ақпараттарға төнген қауіп-қатерлердің мүмкіндігі күшеюде. Сондықтан ақпараттық қауіпсіздік мәселелерін жетілдіру маңызды мәселелердің бірі болып табылады. Ал, ақпараттың қауіпсіздік мәселелерін шешудің бірден-бір жолы ол ақпаратты шифрлеу. Шифрлеу қоғамымыздың қызмет етуінде маңызды рөл атқарады. Мысалы, бүгінгі таңда миллиондаған адамдар күн сайын онлайн сатып алу процесіне, web-сайттар мен электронды пошта, WhatsApp хабар алмасу қосымшасына жүгінеді. Ондағы қолданылатын төлем картасы туралы ақпарат желіде кез-келген уақытта ұрлануы мүмкін. Сондықтан осы процестің іске асырылуын түсіну үшін шифрлеудің негізгі мәселелерін білу маңызды болып табылады. Мақалада шифрлеу жүйесінің негізгі жүзеге асырылу мәселесін түсіну үшін Цезарь әдісі мен Python программалау ортасында Fernet кітапханасының көмегімен мәтінді шифрлеу(дешифрлеу) мысалы қарастырылған. Мақаланың негізгі мақсаты – мәтінді шифрлеу мәселелері бойынша білім алушылардың базалық білімін қалыптастыру. Мақалада қарастырылған мысалдар болашақ информатика мұғалімдерінің шифрлеу мәселелері бойынша теориялық білімдерін және практикалық дағдыларын қалыптастыруға, сонымен қатар алдағы уақытта машиналық оқытуда ақпараттық қауіпсіздіктің мүмкіндіктерін зерттеуге мүмкіндік береді.

Кілтті сөздер: ақпараттық қауіпсіздік, шифрлеу, дешифрлеу, fernet кітапханасы, Цезарь әдісі.

Кіріспе

Белгілі бір құндылықты білдіретін ақпарат қорғауға жатады. Ақпараттың құндылығын анықтау кезінде өзектілігі, бұл ақпараттың иесіне қажеттілігі, жоғалған жағдайда қалпына келтіру сияқты мәселелер маңызды болып табылады.

Ақпаратты қорғау деп ақпараттық қауіпсіздіктің қажетті деңгейін қамтамасыз ету мақсатында іс-шараларды жүзеге асыру үшін қажетті құралдар мен әдістерді қолдануды айтамыз [1]. Электронды-есептеуіш машиналардың хроноологиясы сияқты ақпараттың қауіпсіздігінің даму жүйесін бірнеше кезеңге бөлуге болады [2]:

1 деңгей – 1816 жылға дейінгі кезең. Бұл кезең ақпараттық коммуникацияның табиғи құралдарын пайдаланумен сипатталады.

2 деңгей – 1816 ж.ж..– 1935 ж.ж. дейінгі кезең. Бұл кезең электр және радиобайланыс құралдарының пайда болуымен пара пар. Радиобайланыстың кедергіден қорғалуын қамтамасыз ету үшін хабарламаны (сигналды) шуылға төзімді кодтауды пайдаланумен байланысты.

3 кезең. – 1935 ж.ж. – 1946 ж.ж. дейінгі кезең. Радиолокациялық және гидроакустикалық құралдардың пайда болуымен байланысты. Мұндағы ақпараттық қауіпсіздікті қамтамасыз етудің негізгі жағдайы техникалық құралдарды пайдаланумен байланысты.

4 кезең – 1946 ж.ж. – 1965 ж.ж. Электронды-есептеуіш машиналардың пайда болуымен байланысты. Ақпараттық қауіпсіздікті негізгі мәселелері ақпаратты өңдеу құралдарына қол жетімділікті шектеумен байланысты болды.

5 кезең – 1965 ж.ж. – 1973 ж.ж. Жергілікті желілердің пайда болуымен байланысты. Бұл кезеңде ақпараттық қауіпсіздікті негізгі мәселелері ақпаратты өңдеу құралдарына қол жетімділікті шектеумен байланысты болды.

6 кезең – 1973 ж.ж. – 1985 ж.ж. мобильді коммуникациялық құралдардың пайда болуымен байланысты. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жаңа критерийлер қажет болды. Осы мақсатта қауіпсіздік қамтамасыз ететін ережелер, стандарттар, ақпараттық құқық пайда болды.

7 кезең – 1985 ж.ж. қазіргі кезге дейін. Ауқымды ақпараттық-коммуникациялық желілердің пайда болуымен байланысты. Мұндағы негізгі мәселелерді шешу үшін ақпараттық қауіпсіздіктің макрожүйелерін құру қажеттілігі туындайды.

Білім беру жүйесіндегі ақпараттық қауіпсіздік мәселелерін көптеген Отандық және шетелдік ғалымдар өздерінің зерттеу жұмыстарында қарастырған. Атап айтқанда, М. Бакиев (Ақпараттық қауіпсіздік негіздері),

Актаева А. У. (Ақпараттық қауіпсіздік және қорғау), Устинова Л. В. (Ақпараттық қауіпсіздік және ақпаратты қорғау), Жумагулова С. К. (Ақпараттық қауіпсіздік және ақпаратты қорғау), Алмухамбетов С. С. (Кәсіптік оқытуда ақпараттық қауіпсіздік және ақпаратты қорғау технологиясы), Сәрсенбек М. Б. (Корпоративтік желілердегі ақпараттық қауіпсіздік тәуекелдерін бағалау тәсілдерін талдау), Акимбеков Е. Т. (Кәсіпорынның ақпараттық қауіпсіздігін ұйымдастырудың физикалық қағидалары) және т.б.

G. Shaoyun «The practice of the college students' network security quality education» мақаласында ақпараттық қауіпсіздікті оқыту режимі, желіні құру қадамдарды қарастырылған [3], ал R.Randhir-ң «Use of social media for improving student engagement at université des mascareignes» мақаласында әлеуметтік желілердің артықшылықтары, мәселелері, сонымен қатар оны білім беру жүйесінде қолдану мүмкіндіктері сипатталған [4].

Қазіргі уақытта ақпаратты қорғау үшін криптология әдістері кеңінен қолданылады. Криптология криптография мен криптоанализ мәселелерін қамтиды.

Оқу процесінде теориялық материалмен қатар практикалық тапсырмаларды қандай ортада жүзеге асыру маңызды болып табылады. Оқу ортасы ретінде Excel, Mathcad, Matlab, Python және басқа бағдарламалау орталарын пайдалануға болады. Бұл мақалада біз MS Excel және Python орталарында криптографиялық есептерді шешуді ұсынамыз.

Зерттеу әдістері

Болашақ информатика мұғалімдерін даярлау барысында ақпараттық технологиялардың күн сайын дамуына байланысты білім беру бағдарламасы жыл сайын жаңартылып отыратыны барлығымызға айқын. Сол сияқты ақпараттық қауіпсіздік бойынша ондағы қарастырылатын мәселелер жыл сайын жаңартылып отырады. Сондықтан ақпараттық қауіпсіздік бойынша заман талабына сай машиналық оқытудағы, бұлттық технологияларда, аппараттардың соңғы нүктесіндегі ақпараттың қауіпсіздігі қарастырылады.

Л. Н. Гумилев атындағы Еуразия ұлттық университетінің «5В011100 – Информатика», «6В01511 – Информатика мұғалімдерін даярлау» білім беру мазмұнында ақпараттық қауіпсіздікке байланысты арнайы пән ендірілген. Ал, біздің негізгі мақсатымыз – заманауи техника мен технологияларға байланысты ақпараттық қауіпсіздік бойынша білім алушылардың білімін жетілдіру.

Зерттеу жұмысымыздың міндеттерінің бірі – ақпараттық қауіпсіздік саласында қолданылатын криптографияның негізгі сұрақтарын қарастырумен байланысты.

Себебі ақпараттық қауіпсіздікке тоқталу барысында ең алдымен криптографияның мәселелері қарастырылады. Криптография мәселелерін қарастыру барысында Цезарь шифры, матрицалы шифр, Виженер шифры сияқты сұрақтар қарастырылса, заманауи талаптарға сай гомоморфты шифрлеу қарастырылады.

Гомоморфты шифрлау дегеніміз– пайдаланушыларға шифрланған мәліметтерді алдымен шифрын шешпей-ақ есептеулерді орындауға мүмкіндік беретін шифрлау түрі [5]. Гомоморфты шифрлаудың мынадай түрлерін қарастырайық [6]:

Ішінара гомоморфты шифрлау қосу немесе көбейту сияқты қақпаның тек бір түрінен тұратын схемаларды бағалауды қолдайтын схемаларды қамтиды.

Жартылай гомоморфты шифрлау схемалары қақпалардың екі түрін бағалай алады, бірақ тек тізбектердің ішкі жиыны үшін.

Қабатты толық гомоморфты шифрлау шектеулі (алдын ала анықталған) тереңдіктегі қақпалардың бірнеше түрінен тұратын ерікті схемаларды бағалауды қолдайды.

Толық гомоморфты шифрлау (FHE) шексіз тереңдіктегі қақпалардың бірнеше түрінен тұратын ерікті схемаларды бағалауға мүмкіндік береді және гомоморфты шифрлаудың ең күшті түсінігі болып табылады.

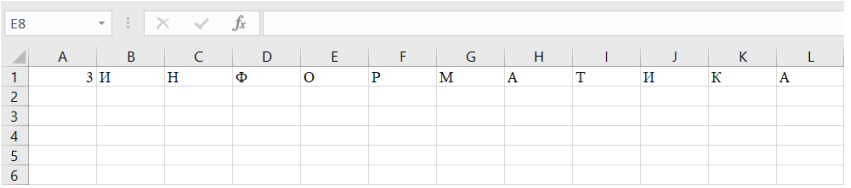
Талқылау

Ең алдымен Цезарь шифрлеуін MS Excel ортасында жүзеге асырылуын қарастырайық [7].

MS Excel ортасында келесі мәліметтерді енгізейік:

A1 ұяшығында кілт орнатайық, оның мәні 3-ке тең.

B1: L1 диапазонына «ИНФОРМАТИКА» сөзін енгізейік.



Сурет 1 – Кілт тағайындау

B2 ұяшығына КОДСИМВ() формуласын енгіземіз. Аргументы функции терезесін ашамыз да, енгізу жолына B1-мәнін енгіземіз. Нәтижесінде B2 ұяшығында 200-ге тең «И» код символы пайда болады. B2 ұяшығының мазмұнын C2: L2: диапазонына көшіреміз.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	3	И	Н	Ф	О	Р	М	А	Т	И	К	А	
2		200	205	212	206	208	204	192	210	200	202	192	
3													
4													
5													

Сурет 2 – Шифрлеу нәтижесі

«Я» символының кодын анықтайық, себебі ол орыс алфавитіндегі соңғы әріп болып табылады. Ол үшін М1 ұяшығына «Я» символын енгізейік. М2 ұяшығына В2 ұяшығының мазмұнын көшіреміз. Я символының коды пайда болады.

Орыс алфавитінің әріп санын анықтаймыз, яғни 223-191=32. «А» әрпі 192-191=1, «В» әрпі 193-191=2 тағы сол сияқты «Я» әрпі 223-191=32 тең болады.

Цезарь әдісімен алынатын шифромәтінді В3: L3 диапазонына енгізейік. Ол үшін В3 ұяшығына =СИМВОЛ(В2+3) енгіземіз. Нәтижесінде 3-ші суреттегідей нәтижеге қол жеткіземіз.

	A	B	C	D	E	F	G	H	I	J	K	L
1	3	И	Н	Ф	О	Р	М	А	Т	И	К	А
2		200	205	212	206	208	204	192	210	200	202	192
3		Л	Р	Ч	С	У	П	Г	Х	Л	Н	Г
4												
5												

Сурет 3 – Шифромәтін

Нәтижесінде ЛРЧСУПГХЛНГ шифромәтін алынды.

Алынған шифромәтін бойынша ағымдық мәтінді анықтайық, яғни алынған шифромәтіннің криптоталдауын жүргізейік.

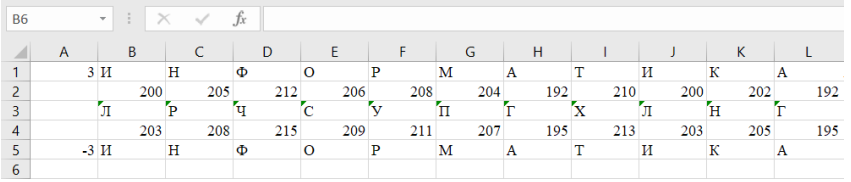
Ол үшін ағымдық мәтін ретінде шифромәтінді қолданылып, 29 кілтін қолдану қажет, себебі -3 mod 32=29.

В4 ұяшығына =КОДСИМВ(В3) формуласын енгізейік те барлық диапазон бойынша көшіріп шығайық.

	A	B	C	D	E	F	G	H	I	J	K	L
1	3	И	Н	Ф	О	Р	М	А	Т	И	К	А
2		200	205	212	206	208	204	192	210	200	202	192
3		Л	Р	Ч	С	У	П	Г	Х	Л	Н	Г
4		203	208	215	209	211	207	195	213	203	205	195
5												

Сурет 4 – Криптоталдау нәтижесі

B5 ұяшығына келесі формуланы енгізейік: =СИМВОЛ(B4+A5). Нәтижесінде 5-ші суреттегідей ағымдық мәтінге қол жеткіземіз.



	A	B	C	D	E	F	G	H	I	J	K	L
1	3	И	Н	Ф	О	Р	М	А	Т	И	К	А
2		200	205	212	206	208	204	192	210	200	202	192
3		Л	Р	Ч	С	У	П	Г	Х	Л	Н	Г
4		203	208	215	209	211	207	195	213	203	205	195
5	-3	И	Н	Ф	О	Р	М	А	Т	И	К	А
6												

Сурет 5 – Ағымдық мәтінді алу

Енді осы мәтіннің шифрлеуін Python программалау ортасында жүзеге асырайық.

Python программалау ортасында мәтінді шифрлеу үшін fernet кітапханасы қолданылады.

Fernet кітапханасы – криптографияның аутентификациялық симметриясын («құпия» кілт көмегімен) жүзеге асырады.

Криптографиялық пакеттің fernet модулінде кілтті генерациялау, ашық мәтінді шифрлау және дешифрлау үшін кірістірілген функциялар бар. Fernet модулі шифрланған деректерді кілтсіз өңдеуге немесе оқуға болмайтындығына кепілдік береді [8].

Fernet модулінде мынадай әдістер қолданылады:

gener_key() : Бұл әдіс жаңа fernet кілтін жасайды. Кілтті қауіпсіз сақтау керек, өйткені ол шифрлық мәтінді шешудің ең маңызды құрамдас бөлігі болып табылады. Егер кілт жоғалса, пайдаланушы хабарламаның шифрын аша алмайды. Сондай-ақ, хакер кілтке қол жеткізсе, олар деректерді оқып қана қоймай, жалған деректерді жасай алады.

encrypt(data): Ол әдіске параметр ретінде берілген деректерді шифрлайды. Бұл шифрлаудың нәтижесі «Fernet таңбалауышы» ретінде белгілі. Ол негізінен шифрленген мәтін болып табылады.

Модульдің параметрлері:

data (bytes) – Шифрланатын ашық мәтін [9].

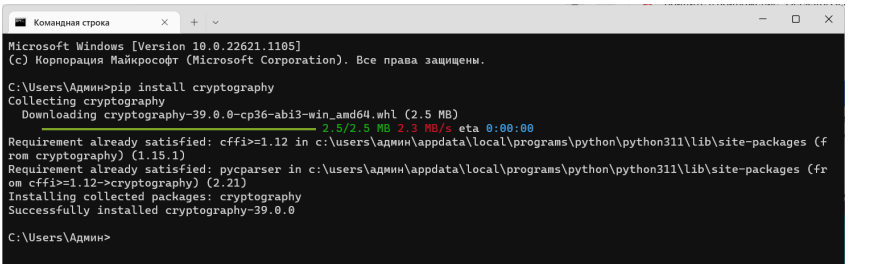
decrypt(token,ttl=None): Бұл әдіс әдіске параметр ретінде жіберілген Fernet байттарын шешеді. Дешифрлеу нәтижесінде бастапқы ашық мәтін алынады.

Параметрлері

token (bytes) – шифромәтінді дешифрлейді;

ttl (int) – Таңдау бойынша шифрды шешу әдісінде екінші параметр ретінде бүтін сан берілуі мүмкін. ttl байттың жарамдылық мерзімін білдіреді.

Криптографиялық модульді қолданбас бұрын оны 7-ші суреттегідей Командалық жолдың көмегімен орнатып аламыз.



Сурет 7 – Cryptography пакетін орнату

Клавиатура арқылы енгізілген мәтінді шифрлеудің программасын қарастырайық [10].

```
// шифрлеу модулін іске қосу
from cryptography.fernet import Fernet
// клавиатура арқылы мәтінді енгізу
str1 =input()
//кілт генерациялау
key = Fernet.generate_key()
// генерацияланған кілтті шифрлеуге тағайындау
fernet = Fernet(key)
// мәтінді шифрлеу
enctex = fernet.encrypt(str1.encode())
// шифромәтінді дешифрлеу
dectex = fernet.decrypt(enctex).decode()
// нәтижесін экранға шығару
print(«Bastapky jol: «, str1)
print(«Shifrlengen matin: «, enctex)
print(«Deshifrlengen matin: «, dectex)
```

Қарастырылған мысалдардың көмегімен «Ақпараттық қауіпсіздік» курсы бойынша мәтінді шифрлеу мәселелерін жылдам, әрі оңай қарастырдық. Мұндағы мысалдар мәтінді шифрлеу ғана емес, сонымен қатар кері шифрлеу(дешифрлеу) мәселелері қарастырылған. Сонымен қатар, мәтінді шифрлеу барысындағы кілттің маңыздылығына тоқталдық. Бұл мәселелер алдағы уақытта қарастырылатын сұрақтардың бірі машиналық оқытудағы ақпараттық қауіпсіздікті жетік түсінуге мүмкіндік береді. Жоғарыда қарастырылған мәселелер білім алушылардың теориялық

және практикалық дағдыларын жетілдіре отырып, ақпараттық қауіпсіздік бойынша базалық білімін қалыптастырады.

Қорытынды

Қарастырылып отырған мақалада Л. Н. Гумилев атындағы Еуразия ұлттық университетінің «5В011100 – Информатика», «6В01511 – Информатика мұғалімдерін даярлау» білім беру бағдарламасының білім алушыларына «Ақпараттық қауіпсіздік» курсы бойынша криптография элементтері қарастырылған. Мұндағы негізгі мәселе білім алушылардың шифрлеу бойынша базалық білімдерін қалыптастыру болып табылады. Ол үшін MS Excel ортасында Цезарь әдісі көмегімен мәтінді шифрлеу және дешифрлеу, сонымен қатар Python программалау ортасында fernet кітапханасы көмегімен мәтінді шифрлеу(дешифрлеу) мысалы қарастырылды. Бұл мәселелер алдағы уақытта Python программалау ортасында машиналық оқытудағы ақпараттық қауіпсіздікті жетік меңгеруге негіз болады.

ПАЙДАЛАНҒАН ДЕРЕКТЕР ТІЗІМІ

1 **Малюк, А. А.** Информационная безопасность : концептуальные и методологические основы защиты информации. – М. : ГЛТ, 2016. – 280 с.

2 **Либкинд, А. С.** «Информационная безопасность – история проблемы и ее решение. – М., 2009. – 20 с.

3 **Shaoyun, G.** «The practice of the college students' network security quality education» // Recent Developments in Mechatronics and Intelligent Robotics. – 2018. – P. 110–114.

4 **Randhir, R.** «Use of social media for improving student engagement at université des mascareignes» // Information Systems Design and Intelligent Applications. – 2019. – P. 11–20.

5 **Варновский, Н. П., Шокуров, А. В.** Гомоморфное шифрование. – 2007. – 27–36 с.

6 **Рябко, Б. Я.** Криптографические методы защиты информации. – М. : ГЛТ, 2013. – 229 с.

7 **Баранова, Е. К.** Криптографические методы защиты информации. – М. : КноРус, 2018. – 288 с.

8 **Златопольский, Д. М.** Основы программирования на языке Python. – М. : ДМК Пресс, 2017. – 284 с.

9 **Любанович, Б.** Простой Python. Современный стиль программирования. – СПб. : Питер, 2016. – 480 с.

10 **Воган, Л.** «Непрактичный» Python : занимательные проекты для тех, кто хочет поумнеть. – СПб. : БХВ-Петербург, 2021. – 464 с.

REFERENCES

1 **Malyuk, A. A.** Informacionnaya bezopasnost': konceptual'nye i metodologicheskie osnovy zashchity informacii . – Moscow : GLT, 2016. – 280 p.

2 **Libkind, A. S.** «Informacionnaya bezopasnost' – istoriya problemy i ee reshenie.– Moscow, 2009. – 20 p.

3 **Shaoyun, G.** «The practice of the college students' network security quality education» // Recent Developments in Mechatronics and Intelligent Robotics. – 2018. – P. 110–114.

4 **Randhir, R.** «Use of social media for improving student engagement at université des mascareignes» // Information Systems Design and Intelligent Applications. – 2019. – P. 11–20.

5 **Varnovskij, N. P., SHokurov, A. V.** Gomomorfnoe shifrovanie. – 2007. – 27–36 p.

6 **Ryabko, B. Ya.** Kriptograficheskie metody zashchity informacii. – Moscow : GLT, 2013. – 229 p.

7 **Baranova, E. K.** Kriptograficheskie metody zashchity informacii – Moscow : KnoRus, 2018. – 288 p.

8 **Zlatopol'skij, D. M.** Osnovy programmirovaniya na yazyke Python. – Moscow : DMK Press, 2017. – 284 p.

9 **Lyubanovich, B.** Prostoj Python. Sovremennyj stil' programmirovaniya. – St. Peterburg : Piter, 2016. – 480 p.

10 **Vogan, L.** «Nepraktichnyj» Python: zanimatel'nye proekty dlya tekh, kto hochet poumnet'. – St. Peterburg : BHV-Peterburg, 2021. – 464 p.

Материал 24.05.23 баспаға түсті.

**М. Серик[1], Д. Ш. Тлеумагамбетова[2]*
[1,2]Евразийский университет имени Л. Н. Гумилева,
Республика Казахстан, г. Астана.
Материал поступил в редакцию 24.05.23.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ НЕКОТОРЫХ ВОПРОСОВ ПО КУРСУ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Сегодня в связи с бурным развитием информационных и коммуникационных технологий и сети Интернет, несмотря на совершенствование мер безопасности, возрастает возможность

угроз информации. Поэтому повышение информационной безопасности является одним из важнейших вопросов. И один из способов решить проблемы информационной безопасности – шифрование. Шифрование играет важную роль в функционировании нашего общества. Например, сегодня миллионы людей ежедневно используют процесс онлайн-покупок, веб-сайты и электронную почту, приложение для обмена сообщениями WhatsApp. Информация платежной карты, используемая в нем, может быть украдена в любое время в Интернете. Поэтому для понимания реализации этого процесса важно знать основы шифрования. В статье приводится пример шифрования (дешифрования) текста с использованием метода Цезаря и библиотеки Fernet в среде программирования Python, чтобы понять основную проблему реализации системы шифрования. Основная цель статьи – сформировать у учащихся базовые знания о шифровании данных. Рассмотренные в статье примеры позволяют сформировать теоретические знания и практические навыки будущих учителей информатики по вопросам шифрования, а также в будущем изучить возможности информационной безопасности в машинном обучении.

Ключевые слова: информационная безопасность, шифрование, дешифрование, библиотека fernet, метод Цезаря.

**M. Serik[1], D. Sh. Tleumagambetova[2]*
[1,2]L. N. Gumilyov Eurasian National University,
Republic of Kazakhstan, Astana.
Material received on 24.05.23.

GUIDELINES FOR TEACHING SOME QUESTIONS ON THE COURSE «INFORMATION SECURITY»

Today, due to the rapid development of information and communication technologies and the Internet, despite the improvement of security measures, the possibility of information threats is increasing. Therefore, improving information security is one of the most important issues. And one of the ways to solve information security problems is encryption. Encryption plays an important role in the functioning of our society. For example, today, millions of people use the online shopping process, websites and email, the messaging app WhatsApp on a daily basis. The payment card information used in it can be stolen at any time on the Internet. Therefore,

to understand the implementation of this process, it is important to know the basics of encryption. The article provides an example of encrypting (decrypting) text using the Caesar method and the Fernet library in the Python programming environment in order to understand the main problem of implementing an encryption system. The main purpose of the article is to form students' basic knowledge about data encryption. The examples considered in the article make it possible to form theoretical knowledge and practical skills of future computer science teachers on encryption issues, as well as to explore the possibilities of information security in machine learning in the future.

Keywords: information security, encryption, decryption, fernet library, Caesar's method.

Теруге 24.05.2023 ж. жіберілді. Басуға 30.06.2023 ж. қол қойылды.
Электронды баспа
7,53 Mb RAM
Шартты баспа табағы 24,7.
Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген З. С. Искакова
Корректорлар: А. Р. Омарова, Д. А. Кожас
Тапсырыс № 4083

Сдано в набор 24.05.2023 г. Подписано в печать 30.06.2023 г.
Электронное издание
7,53Mb RAM
Усл.п.л. 24,7. Тираж 300 экз. Цена договорная.
Компьютерная верстка З. С. Искакова
Корректоры: А. Р. Омарова, Д. А. Кожас
Заказ № 4083

«Toraighyrov University» баспасынан басылып шығарылған
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
8 (7182) 67-36-69
e-mail: kereku@tou.edu.kz
www.vestnik-pedagogic.tou.edu.kz