ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

0148-2963.

16. Abdulkareem, N. M., Abdulazeez, A. M., Zeebaree, D. Q., & Hasan, D. A., "COVID-19 World Vaccination Progress Using Machine Learning Classification Algorithms," Qubahan Academic Journal, Vol.1, No.2, pp.100-105, 2021.

17. Al Dujaili, M. J., Ebrahimi-Moghadam, A., & Fatlawi, A., "Speech emotion recognition based on SVM and KNN classifications fusion," International Journal of Electrical and Computer Engineering, Vol.11, No.2, pp.1259, 2021.

18. Huang, S., Cai, N., Pacheco, P. P., Narrandes, S., Wang, Y., & Xu, W., "Applications of support vector machine (SVM) learning in cancer genomics," Cancer Genomics-Proteomics, Vol.15, No.1, pp.41-51, 2018.

19. X. Luo, Efficient English text classification using selected Machine Learning Techniques, Alex. Eng. J., 60 (3) (2021), pp. 3401-

3409, 10.1016/j.aej.2021.02.009

20. Naeem MZ, Rustam F, Mehmood A, Mui-Zzud-Din, Ashraf I, Choi GS. Classification of movie reviews using term frequency-inverse document frequency and optimized machine learning algorithms. PeerJ Comput Sci. 2022 Mar 15;8:e914. doi: 10.7717/peerj-cs.914. PMID: 35494818; PMCID: PMC9044332.

ӘОЖ 004.056

МОБИЛЬДІ ҚОСЫМШАЛАРДЫҢ ҚАУІПСІЗДІГІН ҚОРҒАУ

Сагинтаев Абат Әлімжанұлы
sagintayev.abat@gmail.com
Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық қауіпсіздік» кафедрасының
1-ші курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – PhD, оқытушы Жеткенбай Лена

Аңдатпа. Қазіргі таңда мобильді қосымшалардың қауіпсіздігі өте маңызды болып табылады. Мобильді құрылғылардағы қосымшалардың қауіпсіздігі пайдаланушы деректерін әртүрлі шабуылдардан, хакерлерден, зиянды программалардан және т.б. манипуляциялардан немесе ұрланудан қорғау процесі. Осы зерттеу жұмысы барысында мобильді қосымшаларды қорғауда қолданылатын тиімді әдістер мен ақпаратты шифрлау алгоритмдері қарастырылды және қазіргі таңдағы танымал алгоритмдерге шолу жасалды.

Кілттік сөздер: ақпараттық қауіпсіздік, шифр, шифрлау алгоритмдері, ашық кілт, жабық кілт.

1. Кіріспе

Ақпараттық қауіпсіздікті қорғау өте маңызды және өзекті мәселеге айналған. Қазіргі таңда смартфондар адамдардың ең көп қолданатын және қажеттіліктерін өтейтін таптырмас құрал болып табылады. Смартфондардың танымал, әрі кең қолданысқа ие болуына әсер еткен әрине мобильді қосымшалар. Бұрын мобильді қосымшалар ойын түрінде дамыған болса, қазіргі уақытта бизнесте мықты маркетингтік құралға айналған. Жалпылай айтқанда, мобильді қосымшалардың қауіпсіздігі дегеніміз мобильді құрылғыларға арналған қосымшаларды зиянды программалардан, әртүрлі хакерлік шабуылдардан, сондай-ақ басқа да қылмыстық манипуляциялар сияқты цифрлық алаяқтықтан кешенді қорғау шарасы, әрі тиімді құралы. Мобильді қосымшалардың құрылымынан бөлек қауіпсіздігін қамтамасыз ету қажеттілігі туындады. Қауіпсіздікті қамтамасыз ету үшін яғни қауіптердің алдын алу немесе болдырмау мақсатында, сондай-ақ деректерді сыртқы шабуылдардан, ішкі шабуылдардан және де ақаулардан қорғау үшін әртүрлі тиімді әдістер мен ақпаратты шифрлау алгоритмдері қолданылады және сөзсіз қолдану қажет.

Негізгі түсініктер

Ақпараттық қауіпсіздік – бұл қарапайым мәтінді немесе хабарламаны ақпаратты оқуға арналған кілті барлардан басқа ешкім оқи алмайтындай етіп қауіпсіздікті қамтамасыз ету [1].

Деректер алынса да, ұрылар (хакерлер) оны оқи алмайды және пайдалана алмайды дегенді білдіреді.

Мобильді қосымшалардың қауіпсіздігі деп зиянды программалар, сондай-ақ басқа да цифрлық алаяқтықтан, сыртқы төнетін қатерлерден мобильді қосымшаларды қорғайтын әдісті айтамыз [2].

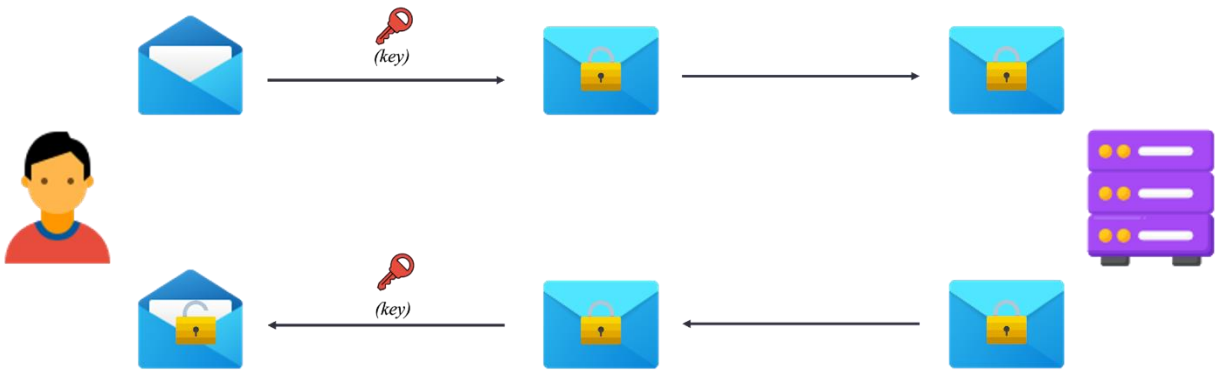
Шифрлау – бұл ақпаратты оқылмайтын түрге (шифрға) түрлендіру процесі, оны тек кілт арқылы оқуға болады. Бұл мобильді қосымшалар мен пайдаланушы деректерін қорғаудың ең тиімді әдістерінің бірі [3].

Кері шифрлау - шифрланған ақпаратты қайта оқуға мүмкін болатындай етіп түсінікті түрге айналдыру процесі.

2. Қауіпсіздікті қамтамасыз ету

Мобильді қосымшаларды қорғауда қолданылатын қауіпсіздік мәселелеріне тоқталып өтейік. Мобильді қосымшаларды қорғаудың маңызды әдісіне көп факторлы аутентификацияны жатқызсақ болады. Бұл әдіс пайдаланушыдан құпия сөзді немесе PIN кодты ғана емес, сонымен қатар саусақ ізі, дауыс, бет-әлпет және т.б. сияқты қосымша деректерді талап етеді. Сондай-ақ, пайдаланушылардың қосымшаның қандай мүмкіндіктеріне қол жеткізе алатынын анықтауға мүмкіндік беретін енуді басқару механизмдері бар. Мысалы, егер қосымша тек компания қызметкерлеріне пайдалануға арналған болса, онда қолданбаны рұқсат етілмеген пайдаланушылар пайдалана алмайтындай етіп орнатуға болады. Сонымен қатар, мобильді қосымшаларды қорғаудың маңызды әдісі – олар жұмыс істейтін қосымшалар мен операциялық жүйені үнемі жаңартып отыру. Жаңартуларда қауіпсіздік осалдығын түзетулер, сондай-ақ қолданбаның қауіпсіздігін жақсартатын жаңа мүмкіндіктер болуы мүмкін. Антивирустық программалар да зиянкестердің пайдаланушының құпия деректеріне қол жеткізу әрекеттерін анықтап бұғаттай алады.

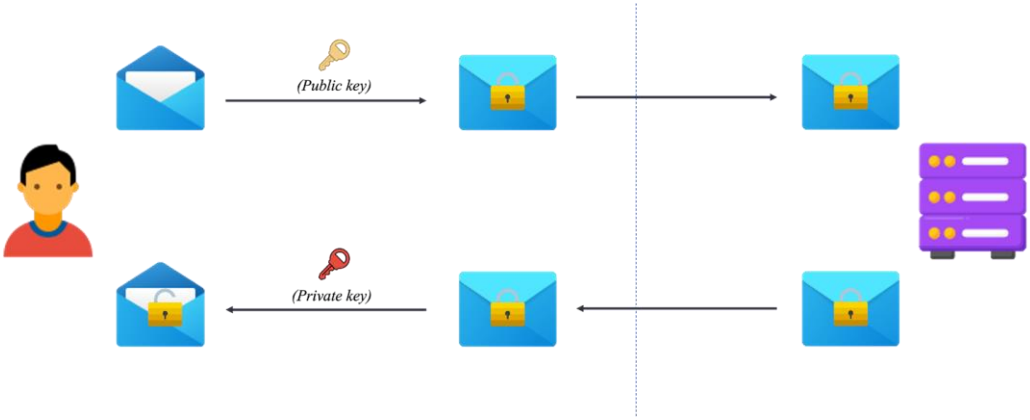
Мобильді қосымшаларды қорғау үшін қолдануға болатын бірнеше шифрлау әдістері бар. Шифрлаудың танымал түрі – ақпаратты шифрлау және шифрын ашу үшін бір кілтті қолданатын симметриялы шифрлау. 1-ші суретте симметриялы шифрлау алгоритмінің сұлбасы келтірілген.



Сурет 1 – Симметриялы шифрлау

Бұл әдіс асимметриялық шифрлауға қарағанда қауіпсіз емес. Дегенмен, мықты шифрлау әдістерін пайдаланған кезде де, шабуылдаушы шифрлау кілттеріне немесе қолданбаның осалдықтарына қол жеткізсе, мобильді қосышаның қауіпсіздігіне қауіп төнуі мүмкін.

Асимметриялық шифрлау, ол ашық және жабық кілттің көмегімен жүзеге асырылады. Ашық кілт ақпаратты шифрлау үшін, ал жабық кілт оны ашу үшін қолданылады. 2-суретте ассимметриялы шифрлауға байланысты сұлба келтірілген.

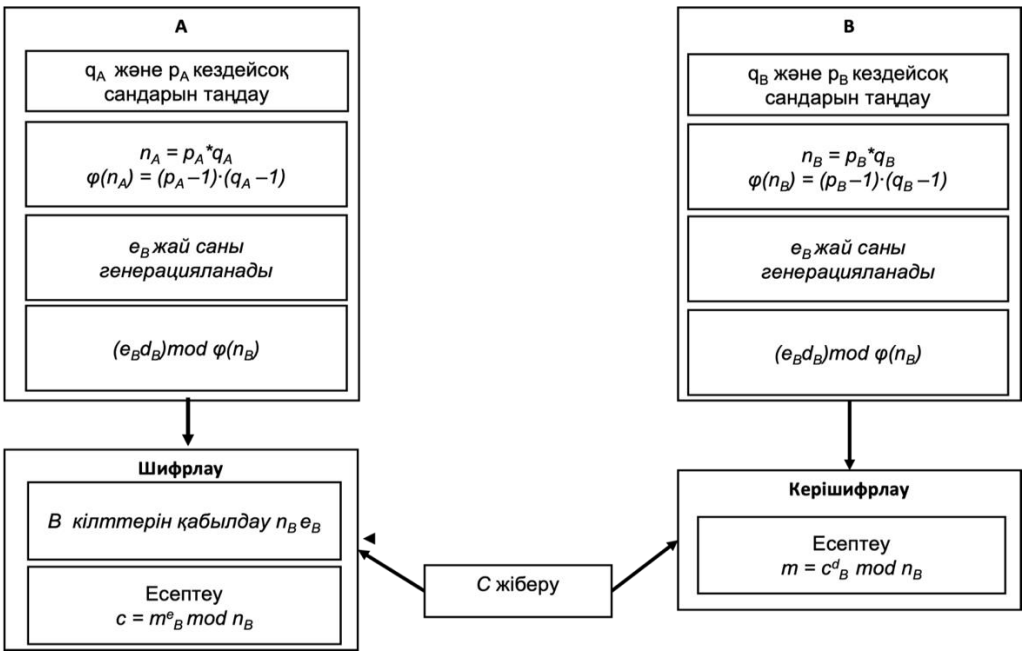


Сурет 2 – Ассимметриялы шифрлау

Бұл қауіпсіздіктің жоғары деңгейін қамтамасыз етеді, өйткені шабуылдаушы ашық кілтке қол жеткізсе де, ол жабық кілтсіз ақпаратты шеше алмайды.

Қолданбаның бұзылуынан барынша қорғауды қамтамасыз ету үшін операциялық жүйе деңгейінде шифрлауды пайдалану маңызды. Сонымен қатар, шифрлау кілттерінің қауіпсіз жерде сақталуын және шабуылдаушыларға қол жетімді болмауын қамтамасыз ету қажет.

Криптожүйелердің дамуымен ең көп таралған ассиметриялық жүйеге RSA-ны жатқызсақ болады. Алгоритмнің RSA деп аталуының себебі, Ривест, Шамир, Адлеман атты өнертапқыштардың аттарымен байланысты. Олардың бастапқы әріптерінен қысқартылып алынған. Бұл криптожүйе ассиметриялы деп аталады. Ассиметриялы криптожуйеде хабарламаны шифрлауға ашық кілт, кері шифрлауға жабық кілт қолданылады. Ашық кілт барлық пайдаланушыларға көрінеді, ал жабық кілт тек тиесілі пайдаланушыға ғана белгілі болады. Хабарламалар шифрланғаннан кейін деректер қорында сақталады. Хабарламалар ашық кілтпен шифрланғаннан соң олар тек тиісті жабық кілтпен кері шифрланады [4]. 3-суретте RSA криптографиялық жүйесінің сұлбасы ұсынылған.



Сурет 3 – RSA криптографиялық жүйесінің сұлбасы

3. Әлемдік компаниялар қолданатын алгоритмдер

Бүкіл әлемге әйгілі Марк Цукерберг негізін қалаған Meta компаниясының бірнеше танымал мобильді қосымшалары, мессенджерлері бар. Соның ішінде барлығымыз күнделікті

хат алмасу үшін қолданатын WhatsApp қосымшасы шифрлау алогритмдерін қолдану арқылы қорғалған. WhatsApp-та «Соңына дейін шифрлау» (end-to-end encryption) алгоритмі қолданылады. Бұл шифрлау алгоритмі сонымен қатар Signal қосымшасында да қолданылады. Мобильді қосымшаларды программалаушылардың айтуынша аталмыш алгоритм 2016 жылдан бастап қолданысқа ене бастаған. WhatsApp қосымшасын қолданушылардың хат алмасуы кезінде шифрлаумен кері шифрлау қолданушының құрылғысының өзінде орындалады. Хабарламаны жібермес бұрын құрылғыда криптологиялық кілт арқылы қорғалады. Әрбір хабарламаны жіберген сайын кілт жаңадан ауысып отырады [3]. Яғни, әйгілі қосымшаның өзі сіздің хабарламаларды оқи алмайды мыс. Демек, хабарламалар Meta компаниясының сервелерінің көмегімен шифр мәтін ретінде жіберіледі. Нәтижесінде сырттан шабуыл жасаушы хакер немесе алаяқтардың ақпаратқа қол жеткізу қаупі өте аз.

Қорытынды

Қорытындылай келе, мобильді қосымшаларды қорғау – бұл пайдаланушылардың қауіпсіздігін қамтамасыз ету және құпия ақпаратты сақтау үшін өте маңызды. Осы мақсатқа жету үшін мобильді қосымшаны жасаушылар пайдаланушының аутентификациясы, қол жетімділікті басқару және шифрлау сияқты әртүрлі қорғаныс әдістерін қолдана алады. Мобильді қосымшалар мен пайдаланушы деректерін қорғаудың ең тиімді әдістерінің бірі болып табылатын шифрлауға ерекше назар аудару керек. Алайда, шифрлаудың күшті әдістерін қолданған кезде де, егер шабуылдаушы шифрлау кілттеріне немесе қосымшаның осалдығына қол жеткізсе, мобильді қосымшалардың қауіпсіздігіне қауіп төнуі мүмкін екенін есте ұстаған жөн. Сондықтан мобильді қосымшаларды барынша қорғауды қамтамасыз ету үшін әзірлеушілер бірнеше қорғаныс әдістерін қолданып, осалдықтарды жою және қауіпсіздік деңгейін жақсарту үшін оларды үнемі жаңартып отыруы керек. Сонымен қатар, пайдаланушылардың мобильді қосымшалардың қауіпсіздігі туралы жеткілікті ақпаратқа ие екендігіне және олардың құпия ақпаратын қорғау үшін шаралар қабылдағанына көз жеткізу маңызды.

Пайдаланылған әдебиеттер тізімі

1. Уикипедия ашық энциклопедиясы https://kk.wikipedia.org/wiki/%D0%90%D2%9B%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D1%82%D1%8B%D2%9B_%D2%9B%D0%B0%D1%83%D1%96%D0%BF%D1%81%D1%96%D0%B7%D0%B4%D1%96%D0%BA Қаралған күні: 19.03.2023 ж.

2. Уикипедия ашық энциклопедиясы https://kk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80 Қаралған күні: 19.03.2023 ж.

3. https://faq.whatsapp.com/820124435853543/?helpref=hc_fnav Қаралған күні: 19.03.2023 ж.

4. Қолданбалы криптология: шифрлау әдістері: Оқулық. – Алматы: Қ. И. Сәтбаев атындағы ҚазҰТЗУ, 2016. 14 – 42 бет, 449 – 456 бет.

ӘОЖ 004.89

СӨЙЛЕУДІ СИНТЕЗДЕУДІҢ СТАТИСТИКАЛЫҚ ӘДІСТЕРІ

Сарсенбаева Азиза Габитовна
azizok_96@mail.ru
Л.Н.Гумилев атындағы Еуразия ұлттық университеті
«Ақпараттық технологиялар» факультеті
«Жасанды интеллект технологиясы» кафедрасының магистранты, Астана, Қазақстан
Ғылыми жетекші – Г.Т. Бекманова

Аңдатпа

Сөйлеуді танумен қатар сөйлеуді өңдеудің маңызды міндеттерінің бірі сөйлеуді синтездеу немесе басқаша айтқанда мәтінді сөйлеуге түрлендіру болып табылады. Ең алғашқы