3 ГІСТОРЫІ КРЫПТАГРАФІІ І ШЫФРАВАННЯ. БЕЛАРУСКАЯ КРЫПТАВАЛЮТА.

Юнга С.Ю., Літаш А.В., Канаваленка І.А.

Беларускі дзяржаўны ўніверсітэт інфарматыкі і радыёэлектронікі
г. Мінск, Рэспубліка Беларусь

Дапіра Т.П. – выкладчык

У рабоце разглядаюцца пытанні з гісторыі зараджэння крыптаграфіі, першых шыфратэкстаў, стварэння першай беларускай крыптавалюты. Раскрываюцца паняцці блокчэйн, крыптавалюта, хэшыраванне. Апісваюцца асаблівасці выкарыстання нацыянальнай мовы ў крыптаграфіі.

Прызначэнне мовы, яе роля – найперш быць сродкам людскіх дачыненняў (зносін), інакш камунікацыі (ад лац.— паведамленне, сувязь, стасункі). Пры кантактах людзі перадаюць адзін аднаму свае думкі, волевыяўленні, пачуцці, уздзейнічаюць адзін на аднаго, дамагаюцца ўзаемаразумення, наладжваюць сумесную працу [1, с.11]. Іншы раз у чалавека ўзнікае патрэба ў канфідэнцыйнасці — калі патрэбна перадаць звесткі так, каб іншы чалавек пры авалоданні гэтымі звесткамі, не змог даведацца пра іх сэнс і змест. Пытаннямі інфармацыйнай бяспекі ў частцы ўтойвання сэнсу пэўнага паведамлення займаецца такая сфера апрацоўкі і пераўтварэння інфармацыі, як шыфраванне, а навука, што вывучае метады шыфравання, называецца крыптаграфія.

Спынімся на асноўных тэрмінах, якімі мы аперыруем у працы:

Крыптаграфія – навука пра метады забеспячэння прыватнасці (немагчымасці чытання інфармацыі староннім) і аўтэнтычнасці (цэласнасці і сапраўднасці аўтарства, а таксама немагчымасці адмовы ад аўтарства) інфармацыі [2].

Крыптааналіз – навука, якая вывучае матэматычныя метады парушэння сакрэтнасці і цэласнасці інфармацыі.

Шыфраванне – тэхналогія кадзіравання і раскадзіравання дадзеных.

Шыфратэкст – вынік прымянення алгарытму для кадзіравання дадзеных з мэтай зрабіць іх недаступнымі для чытання.

Хэш-функцыя – функцыя, якая пераўтварае паведамленне адвольнай даўжыні ў лічбу («скрутка») фіксаванай даўжыні. Для крыптаграфічнай хэш-функцыі (у адрозненні ад хэш-функцыі агульнага прызначэння) складана вылічыць адваротную і нават знайсці два паведамленні з аднолькавым значэннем хэш-функцыі [2].

Крыптаграфія і само шыфраванне выкарыстоўваліся людзьмі на працягу тысячагоддзяў для абароны сваіх сакрэтаў. А ў сучаснасці інфармацыя вельмі важная, бо, як той казаў, хто валодае інфармацыяй, той валодае светам. Так, у Старажытным Рыме была праблема, што ганцы з сакрэтнымі ваеннымі пасланнямі часта падвяргаліся нападам з боку ворагаў. Гэта давала вялізную перавагу перахопнікам, паколькі яны ведалі планы рымскай арміі. Таму неабходна было забяспечыць бяспечную сувязь паміж палкамі. Юлій Цэзар каля 2000 гадоў таму, кіруючы рымскай арміяй, распрацаваў шыфравальны код, у якім замяніў адны літары іншымі. Можна было не хвалявацца за сакрэтнасць інфармацыі, якая перадавалася, бо расшыфраваць паведамленне мог толькі той, хто ведаў табліцу падстановак.

Першы тэкст з элементамі крыптаграфіі быў знойдзены ў грабніцы старажытнаегіпецкага вяльможы, які жыў амаль 4000 гадоў таму. Недзе каля 1900 г. да н. э. пісар Хнумхатэпа занатоўваў жыццё свайго гаспадара ў яго магіле. У самім тэксце ён выкарыстоўваў некалькі незвычайных сімвалаў, якія хавалі сэнс гэтага тэксту. Тады ўжываўся ўжо так званы метад падстаноўкі. З развіццём егіпецкай культуры замена іерогліфаў стала больш распаўсюджанай. Ёсць розныя версіі яе паходжання. Першая версія заключаецца ў тым, што яны хацелі схаваць свае рэлігійныя абрады ад простых людзей. Другая версія – у тым, што перапісчыкі надалі тэксту

нефармальны выгляд, як у наш час юрысты, напрыклад, выкарыстоўваюць спецыфічныя выразы для замены звычайных слоў. Егіпецкая крыптаграфія магла быць спосабам пісара зрабіць уражанне на іншых людзей, каб паказаць, што ён можа выказваць думкі на больш высокім узроўні [3].

Сёння крыптаграфія значна рушыла наперад. У саміх алгарытмах у якасці аперацый, закліканых абцяжарыць лінейны і дыферэнцыяльны крыптааналіз, сталі выкарыстоўваць складаныя матэматычныя канструкцыі. Для вырашэння задачы абароны інфармацыі прапануюцца ўсё новыя механізмы, у тым ліку арганізацыйныя і заканадаўчыя. Развіваюцца прынцыпова новыя кірункі. На стыку квантавай фізікі і матэматыкі развіваюцца квантавыя вылічэнні і квантавая крыптаграфія. У сучасным свеце крыптаграфія знаходзіць мноства розных праяў выкарыстання: у сотавай сувязі, пры падключэнні да Wi-Fi, на транспарце для абароны квіткоў ад падробак, у банкаўскіх аперацыях, для абароны электроннай пошты ад спаму [4].

Неабходна адзначыць, што сучасная крыптаграфія праяўляецца яшчэ ў адным важным аспекце – крыптавалюце. Крыптавалюта – лічбавы актыў, прызначаны для працы ў якасці сродку абмену з выкарыстаннем крыптаграфіі для забеспячэння бяспекі транзакцый і кантролю стварэння дадатковых адзінак валюты [2]. Крыптавалюты класіфікуюцца як падмноства лічбавых валют, а таксама як падмноства альтэрнатыўных валют. Дэцэнтралізаваную крыптавалюту разумеюць як валюту, у якой няма ўнутранага ці вонкавага адміністратара ці якога-небудзь яго аналагу. Сама па сабе крыптавалюта не мае якой-небудзь асаблівай матэрыяльнай або электроннай формы – гэта проста лічба, якая пазначае колькасць дадзеных разліковых адзінак і запісваецца ў адпаведнай пазіцыі інфармацыйнага пакета пратакола перадачы дадзеных, часта нават не падвяргаецца шыфраванню, як і ўся іншая інфармацыя аб транзакцыях паміж адрасамі сістэмы.

Тэхналогія, якая забяспечвае функцыянаванне крыптавалют, а менавіта перадачу сродкаў ад аднаго карыстальніка да іншага, мае назву Blockchain. Блокчэйн – гэта сістэма з блокаў, што паслядоўна стаяць і захоўваюць інфармацыю. Кожны наступны блок утрымлівае ў сабе хэшыраваную інфармацыю папярэдніх блокаў. Гэтая інфармацыя захоўвае ў сабе звесткі аб тым, хто адправіў грашовыя сродкі, хто іх прыняў, а таксама ўсе звесткі аб папярэдніх транзакцыях, у якіх удзельнічалі сродкі, што перадаюцца. Хэшыраванне (з англ. - смецце, блытаніна) - працэс пераўтварэння інфармацыі нявызначанага аб'ёму ў радок з сімвалаў фіксаванай колькасці.

Існуюць розныя тыпы хэшыравання. Адзін з самых папулярных – шыфраванне SHA-256. Хэшыраванне дазваляе шыфраваць інфармацыю з мэтай абароны транзакцый ад парушальнікаў, якія спрабуюць незаконна атрымаць чужыя сродкі. У пачатку кожнай транзакцыі сістэма правярае інфармацыю аб абодвух удзельніках аперацыі, аналізуе паслядоўнасць блокаў хэшыраванай інфармацыі. Калі ж парушальнік паспрабуе выставіць сябе за атрымальніка грашовых сродкаў, то яму давядзецца змяніць абсалютна ўвесь ланцужок блокаў з інфармацыяй, хэшыраванай раней. Такая ўласцівасць хэш-функцыі, пры якой найменшая змена ў звестках прыводзіць да кардынальнай змены наступных блокаў хэшыраванай інфармацыі, называецца «лавінным эфектам». Такім чынам, хэшыраванне прадухіляе магчымасць крадзяжу сродкаў [5].

Беларусь не адстае ад сучаснага свету, і ўжо ў 2017 годзе з'явілася першая айчынная крыптавалюта, якая атрымала назву Талер (на англ. Taler, скароч. TLR). Такая назва прапаноўвалася ў пачатку 1990-х гадоў для ўведзенай тады беларускай грашовай адзінкі. Паходзіць найменне ад старажытнай чаканай срэбнай манеты, якая хадзіла на беларускіх землях у 16-19 стагоддзях. Назва для грашовай адзінкі прынята не была, аднак яна была ўзятая беларускімі аўтарамі і прыменена да крыптавалюты. Стваральнікамі Талера з'яўляюцца два беларусы: Дзяніс Лаўнікевіч, прафесійны журналіст і эканамічны аглядальнік, а таксама Сяргей Лаўрыненка, IT- менеджар. Першая транзакцыя Талера прайшла 13 верасня 2017 года. Гэта дата прынята за дзень нараджэння першай беларускай крыптаманеты. Усяго эмісія Талера складае 23,333,333 манеты. Гэтая крыптавалюта з'яўляецца першым крокам у заяве беларускай біржы на сусветнай арэне. Сёння здзяйсняюцца аперацыі з айчыннай крытавалютай, аднак яе курс не заўсёды стабільны. Хоць нестабільнасць любой крыптавалюты – звычайная справа. Мы будзем спадзявацца, што будучыня не толькі дадзенай крыптавалюты і ўсёй біржавой сістэмы Беларусі будзе толькі развівацца і ўмацоўвацца [6].

У заключэнні хочацца сказаць, што мова адыгрывае вельмі важную ролю ў жыцці чалавека. Нацыянальная мова – найважнейшы сродак зносін паміж прадстаўнікамі пэўнага народа, і агульнасць мовы з'яўляецца важнай умовай эканамічнай і палітычнай канцэнтрацыі жыцця грамадства ў канкрэтны перыяд функцыянавання нацыі. На сучасным этапе беларуская нацыянальная мова паспяхова выконвае свае функцыі ў розных сферах зносін паміж людзьмі. У такіх умовах лічым вельмі важным развіваць функцыянаванне роднай мовы ў сучасных запатрабаваных сферах дзейнасці, а менавіта ў пытаннях інфармацыйных тэхналогій, у галіне абароны інфармацыі, індывідуальнай бяспекі і г.д.

Спіс выкарыстаных крыніц:

1. Сцяцко, П. У. Уводзіны ў мовазнаўства: Дапаможнік / П. У. Сцяцко – Гродна: ГрДУ, 2001. – 229 с.

2. Крыптаграфія [Электронны рэсурс]. – Рэжым доступу: https://be.wikipedia.org/wiki/%D0%9A%D1%80%D1%8B%D0%BF%D1%82%D0%B0%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F – Дата доступу: 04.04.2022.

3. Криптография и защищённая связь: история первых шифров [Электронны рэсурс]. – Рэжым доступу: https://habr.com/ru/post/321338/ – Дата доступу: 04.04.2022.

4. История криптографии [Электронны рэсурс]. – Рэжым доступу: https://ru.wikipedia.org/wiki/История_криптографии#Кр – Дата доступу: 04.04.2022.

5. Криптография в блокчейнах»: о хеш-функциях, ключах и цифровых подписях [Электронны рэсурс]. – Рэжым доступу:]. https://habr.com/ru/company/bitfury/blog/327272/ – Дата доступу: 04.04.2022.

6. Криптовалюта TLR : белорусский талер – имеет ли право на «жизнь» [Электронны рэсурс]. – Рэжым доступу: https://kaktotak.by/vsego-ponemnogu/kriptovaliuta-tlr-belorusskii-taler-imeet-li-pravo-na-zhizn – Дата доступу: 04.04.2022.