УДК 811.111'276.4

Л. П. Мудрак,
аспірант
(Національний педагогічний університет імені М. П. Драгоманова, м. Київ)

З ІСТОРІЇ ВИНИКНЕННЯ ТАЄМНОЇ ПИСЕМНОСТІ

У статті з'ясовано актуальність проблеми захисту інформації та її зв'язок з різноманітними сферами людської діяльності. Досліджено історію виникнення криптографії та криптоаналізу, розглянуто способи шифрування давніх цивілізацій. Наведено приклади використання шифровок у Біблії. Окреслено внесок арабів у становлення криптоаналізу та роль католицької церкви у подальшій розробці та вдосконаленні шифрів.

Проблема захисту інформації шляхом перетворення, яке виключає доступ сторонніх осіб до її джерела, хвилює людський розум із давніх-давен. Дослідження розвитку людського суспільства, відокремлено від постійного потягу до таємниць, неможливе. Споконвіків не існувало більшої цінності, ніж інформація. Політики, військові, священики, торговці, письменники і вчені тисячоліттями працювали над розвитком науки про секрети, постійно вдосконалюючи свої досягнення. Не існує жодної держави або навіть маленької спільноти людей, які б не мали власних таємниць, адже вони (таємниці) є запорукою перемоги та успіху, основою науки, техніки і політики будь-якої людської формації.

Із зародженням людської цивілізації виникла потреба повідомляти інформацію одним людям так, щоб вона не була відомою іншим. До тих пір, поки люди використовували для передачі даних винятково голос і жести, зробити це зазвичай не вимагало великих зусиль – потрібно було лише виключити з безпосереднього оточення тих, для кого ці повідомлення не були призначені. Проте іноді зовнішні фактори накладали на поведінку співрозмовників певні обмеження, що не дозволяли їм сховатися від сторонніх вух і очей для проведення конфіденційної бесіди. Тому в подібних умовах почали використовувати систему кодованої мови або жестів для передачі таємної інформації. У різних ситуаціях застосовувалися різноманітні засоби – від окремого таємного знака, який повідомляв про певну подію, до розвинених секретних мов, що дозволяли виражати думки практично будь-якої складності. Потрібно зазначити, що це була по своїй суті друга сигнальна система в мініатюрі, призначена для передачі обмеженого набору відомостей і відома, як правило, лише невеликій групі людей; частина альтернативної мови, яка поклала початок розвиненому пізніше мистецтву таємно передавати повідомлення.

Звичайно, використання розвиненої "секретної" мови для захисту передачі даних надає набагато більше свободи в комунікації, ніж кілька таємних знаків, про які учасники домовилися напередодні, однак цей шлях має й набагато більші вимоги. Простежити за всіма учасниками процесу завжди важко, і рано чи пізно кодована мова стане зрозумілою тим, від кого намагаються приховати справжній зміст розмови. У цьому випадку виникає необхідність заміни, розробки досить потужної мови, навчити якої потрібно велику кількість людей, що виконати досить важко, а зробити це оперативно навіть неможливо. Тому такий підхід до проблеми може бути доречним тільки в особливих випадках, коли тому сприяють обставини. Наприклад, він використовувався американцями під час Другої світової війни: кораблі ВМФ США здійснювали зв'язок мовою нечисленного й компактно проживаючого індійського племені. На кожному кораблі було кілька індіанців-"шифрувальників"; у супротивника не було практично ніяких шансів роздобути собі такого "криптографа" [2].

Із виникненням писемності завдання забезпечення таємності та дійсності переданої інформації стало особливо актуальним. Звичайно ж, повідомлення, передане словесно або показане жестами, є доступним для сторонньої особистості тільки в той короткий проміжок часу, поки воно "на шляху" до потрібного адресата, а його авторство та відповідність змісту не повинні викликати ніяких сумнівів, тому що одержувач інформації бачить свого співрозмовника. Інша справа, коли повідомлення записане, воно вже живе окремим життям і прямує до цілі своїм власним шляхом. Записані на папері дані існують у матеріальному світі більш тривалий проміжок часу, і у людей, які бажають ознайомитися з їх змістом незалежно від волі відправника та одержувача, з'являється набагато більше шансів зробити це. Тому саме після виникнення писемності, що є не чим іншим, як системою кодування мови, з'явилося мистецтво тайнопису, мистецтво "таємно писати" – набір методів, призначених для секретної передачі записаних повідомлень від однієї людини іншій [2]. Система передачі повідомлення, зміст якого приховується за допомогою шифру, називається шифруванням. Головною метою тайнопису, кодування або шифрування є прагнення зберегти інформацію недоступною для сторонніх людей. Основне завдання – приховати, замаскувати, записати повідомлення таким чином, щоб його зміст був незрозумілим для інших [6: 7].

Дані про перші способи тайнопису досить уривчасті. Тому метою цієї статті є дослідження виникнення та історії розвитку криптологічного мистецтва. Як уже зазначалося раніше, перші

способи захисту записаної інформації з'явилися, швидше за все, з моменту виникнення самої писемності. Найбільш простим і дотепер уживаним способом приховування інформації були конверти або печатки на сувоях, не розкривши які неможливо було довідатися про зміст повідомлення. Однак це був досить примітивний спосіб, який не міг зберегти безпеку переданої інформації, а скоріше засвідчував факт порушення конфіденційності третіми особами. Спроби приховати інформацію ще в стародавньому світі призвели до виникнення перших систем тайнопису. Більшість дослідників вважають, що починати дослідження потрібно з Давнього Єгипту. Яскравим прикладом є написи на гробницях знатних людей, які лише в окремих місцях складалися з незвичайних ієрогліфічних символів замість більш звичних ієрогліфів. У такий спосіб переписувачі не прагнули ускладнити читання тексту, а лише намагалися додати йому більшої важливості та значущості. Ієрогліфи Давнього Єгипту дійсно включали, хоча й не в повній формі, два важливих елементи – таємність і перетворення та переробку листа, які є основними атрибутами криптографії.

Точних дат і достовірних даних про тайнопис у стародавності ніхто не наводить. Відомо, наприклад, що в Давній Греції голову раба голили, писали на ній, чекали, до поки волосся знову відростало, після чого відправляли з дорученням до адресата. Час був такий – відстані більші, швидкості малі. Відголосок цієї історії можна зустріти в "Гіперболіаді інженера Гаріна" Олексія Толстого, де текст нанесли на спину хлопчика [4]. Якщо ж посланець був надійний і навіть під катуваннями не видав би повідомлення, то його доповідь могла бути і усною. Знавцям поезії також добре відомий досить широко використовуваний у той час такий засіб тайнопису, як акровірш, у якому приховуване повідомлення утворюють перші букви віршованих рядків [3: 11].

Цікаво, що в далеку давнину тайнопис вважався одним із 64-х мистецтв, яким треба було володіти як чоловікам, так і жінкам. Відомості про способи шифрування листа можна зустріти вже в документах давніх цивілізацій Індії та Месопотамії. Серед найпростіших – написання знаків не один за одним, а розкидання їх за певними правилами. Один із найстаріших шифрованих текстів з Месопотамії – це табличка, написана клинописом, яка повідомляє рецепт виготовлення глазурі для гончарних виробів. Для його написання були використані рідко вживані клинописні знаки, ігнорувалися деякі голосні та приголосні, а також вживалися числа замість імен. Шифровані тексти Давнього Єгипту – це найчастіше релігійні тексти та медичні рецепти.

Відомо також, що у шумерів, вавилонян і ассирійців релігійні та наукові настанови давалися переважно в усній формі. Найважливіша інформація передавалася з вуст у вуста тільки довіреним особам. "Ми не знайдемо, – говорив Жорж Контей, відомий французький археолог, про ассиро-вавилонську літературу, – жодного твору навчально-настановчого характеру, у якому б повністю викладалася відповідна галузь знання. Жерці намагалися зробити так, щоб доступними для народу були тільки такі твори, які вимагали коментарів для тлумачення їхнього прихованого змісту" [6: 8].

Найбільш повні та достовірні відомості про шифри відносяться до Давньої Греції. Як правило, у древні часи використовувалися так звані шифри заміни та шифри перестановки. Історичним прикладом шифру заміни є шифр Цезаря (I століття до н.е.), описаний істориком Давнього Риму Свєтонієм [1: 6]. Гай Юлій Цезар використовував у своєму листуванні шифр власного винаходу. Якщо проводити паралель із сучасною російською мовою, то він полягав у наступному. Виписувався алфавіт: А, Б, В, Г, Д, Е, ..., потім під ним виписувався той же алфавіт, але зі зміщенням на 3 букви вліво. При зашифровуванні буква А замінялася буквою Г, Б замінялася на Д, Б – на Ї і так далі. Так, наприклад, слово "РИМ" перетворювалося на слово "УЛП". Одержувач повідомлення "УЛП" шукав ці букви в нижньому рядку й по літерах над ними відновлював вихідне слово "РИМ". Ключем у шифрі Цезаря є величина зміщення 3 нижнього рядка алфавіту. Спадкоємець Юлія Цезаря – Цезар Август – використовував той же шифр, але із ключем зміщення 4. Слово "РИМ" він у цьому випадку зашифрував би у буквосполучення "ФМР".

А. Вінокуров вважає, що з висоти досягнень сучасної криптографії шифр Цезаря абсолютно примітивний, однак для того часу, коли вміння читати та писати було рідкісним винятком, його криптостійкості цілком вистачало. Використання шифру вирішувало проблему таємності переданого повідомлення, а проблема дійсності та правдивості відомостей вирішувалася практично сама собою: по-перше, для людини, яка не знала шифр, було неможливо внести осмислені зміни в зашифровані повідомлення, що носили винятково текстовий характер, а зміни, внесені навмання, призводили до того, що після розшифрування отримувався безглуздий набір букв; по-друге, практично до ще зовсім недавніх щодо історичних вимірів часів відправлялися повідомлення, які записувалися від руки, а кожна людина має свій індивідуальний, властивий тільки їй почерк, який дуже важко відтворити комусь іншому; запам'ятати почерк навіть декількох десятків найбільш важливих своїх кореспондентів не вимагало великих зусиль.

Існують також листи Гая Свєтонія до Цицерона та близьких родичів про домашні справи. Якщо потрібно було повідомити що-небудь негласно, то автор користувався тайнописом, тобто міняв букви так, щоб із них неможливо було скласти жодного слова. Для того, щоб розібрати та прочитати їх, необхідно читати щоразу четверту букву замість першої, наприклад, D замість А і так далі. Це означає, що кожна буква шифровки замінялася четвертою від неї за рахунком: А—D, або D замість А.

Повідомлення сенату: VENI VIDI VICI, тобто ПРИЙШОВ, ПОБАЧИВ, ПЕРЕМІГ, зроблене Цезарем після одноденної війни з понтійським царем Фарнаком, виглядало б шировкою SBKF SFAF SFZF [2].

Давньогрецький полководець Еней Тактика (IV століття до н.е.) також залишив значний слід в історії розвитку криптології. Помітним внеском Енея в криптографію є запропонований ним так званий книжковий шифр, описаний у творі "Про оборону укріплених місць". Еней запропонував проколювати малопомітні дірки в книзі або в іншому документі над буквами (або під ними) секретного повідомлення. Цікаво зазначити, що в Першій світовій війні німецькі шпигуни використовували аналогічний шифр, замінивши дірки на крапки, які наносилися симпатичним чорнилом на букви газетного тексту. Книжковий шифр у сучасному вигляді має дещо інший вигляд. Його сутність полягає в заміні літер на номер рядка та номер цієї букви у рядку на заздалегідь обумовленій сторінці певної книги. Ключем такого шифру є книга та зазначена сторінка в ній. Цей шифр виявився "довгожителем" і застосовувався навіть у часи Другої світової війни.

Уже тоді шифрована кореспонденція використовувалася не тільки полководцями, але й церквою і вченими. Жерці шифрували тексти віщунів, а вчені – свої відкриття. Наприклад, в Е. Шюре в книзі "Великие посвященные" зустрічається фраза про те, що "с великим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свое учение иначе, как тайными знаками и под разными символами".

Навіть у Біблії можна знайти приклади шифровок, хоча мало хто це помічає. У книзі пророка Ієремії (25, 26) читаємо: "...а цар Сессаха вип'є після них". Такого царя або царства не було – невже помилка переписувача? Ні, просто інколи священні іудейські тексти шифрувалися простою заміною. Замість першої літери алфавіту писалася остання, замість другої – передостання і так далі. Цей давній метод шифрування називався атбаш. Читаючи за ним слово СЕССАХ, мовою оригіналу отримуємо слово ВАВИЛОН, і зміст біблійного тексту стає зрозумілим навіть невіруючому в істинність писання.

Одна з найвідоміших "криптограм" у Біблії пов'язана з історією про те, як у розпал бенкету у вавилонського царя Валтасара людська рука стала писати на стіні лиховісні слова: "міні, текел, фарес". Однак таємниця полягає не в тому, що означають ці слова.

Самі слова "міні", "текел" і "фарес" запозичено з арамейської мови, схожої до давньоєврейської, і означають "обчислив", "зважений" і "розділено". Коли Валтасар викликав до себе пророка Данила, останній без особливих зусиль прочитав напис і розтлумачив ці три слова: "міні – вирахував Бог царство твоє й поклав кінець йому; текел – ти зважений і знайдений дуже легким; фарес – розділене царство твоє й віддане мідянам і персам" [5: 118].

Напис "міні, текел, фарес" може також означати назви грошових одиниць – міна, текел (1/60 міни) і фарес (1/2 міни). Їх перерахування саме в такій послідовності символізує катастрофу Вавилонської імперії.

Девід Кан стверджує, що в Європі криптографія перебувала в стані стагнації аж до початку епохи Відродження. Шифросистеми, що широко використовувалися на той час, були дуже прості – фрази писалися по вертикалі або у зворотному напрямку, голосні замінялися крапками, використовувалися іноземні алфавіти (наприклад, давньоєврейський та вірменський), кожна буква відкритого тексту замінялася буквою, що слідувала за нею. Відомий також ряд знакових шифрів, у якому літери відкритого тексту заміняються спеціальними знаками. Таким є шифр Карла Великого, що застосовувався в IX столітті н. е. У відомому так званому "єврейському шифрі" заміна літер здійснюється за методом *підстановки*, порядок якої визначається так: алфавіт розподіляється на дві половини, букви другої половини пишуться під буквами першої у зворотному порядку. Літери тексту заміняють тими, які стоять із ними в парі [5].

Протягом багатьох років криптологія потерпала від хвороби, що збереглася до пізніших часів, а саме: багато людей переконані у тому, що криптографія та криптоаналіз, які є складовими частинами криптології, являють собою різновид чорної магії [5: 119].

З перших днів свого існування криптографія мала на меті приховати зміст важливих розділів письмових документів, які мали відношення до таких сфер магії, як гадання та заклинання. В одному з рукописів про магію, що датується III століттям н.е., використовується шифр з метою приховування важливої частини чаклунських рецептів. Криптографія часто-густо перебувала на службі магії в часи середньовіччя і навіть в епоху Відродження: за допомогою шифрів алхіміки утаємничували важливі частини формул отримання "філософського каменю".

Подібність криптографії до магії обумовлювалася й іншими факторами. Крім криптографії, таємничі символи використовувалися в таких зрозумілих лише окремій групі людей галузях магічних знань, як астрологія та алхімія, у яких знаками відкритого тексту було закодовано назви планет або ж хімічних речовин, що мали свій спеціальний знак. Як і зашифровані слова, заклинання та магічні формули, начебто "абракадабри", були схожі на нісенітницю, але у дійсності мали приховане значення.

Думка про те, що криптоаналіз є за своєю природою чорною магією, ґрунтується також і на поверхневій схожості із гаданням. Отримання справжнього змісту із шифротексту повідомлення здавалося точно такою ж справою, що й одержання знань шляхом вивчення розташування зірок і

планет, довжини ліній і місць їхнього перетинання на долоні. Але у жодному із зазначених вище випадків застосування тайнопису підтвердження існування криптоаналізу як науки не було. Час від часу факти дешифрування тексту мали місце. Але наукового обґрунтування не було ні в Єгипті або Індії, ні в Європі аж до 1400 року. Існувала тільки криптографія

Першими відкрили та описали методи криптоаналізу араби. Цей народ створив одну з найрозвиненіших цивілізацій того часу. Арабська наука процвітала. Арабська медицина та математика стали найкращими у світі. Поширилися ремесла. Потужна творча енергія арабської культури, яку іслам позбавив живопису та скульптури, породила плоди на ниві літератури. Широкого поширення набуло складання словесних загадок, ребусів і каламбурів. Граматика набула статусу найголовнішого навчального предмету і містила в собі тайнопис.

Інтерес до криптографії серед арабів почав виявлятися досить давно. У 855 році арабський учений Абу Бакр Ахмед бен-Алі бен-Вахшія ан-Набаті долучив невелику кількість класичних шифроалфавітів до своєї "Книги про велике прагнення людини розгадати загадки давньої писемності". Один такий шифроалфавіт, який називався "дауді" (на честь імені ізраїльського царя Давида), використовувався для шифрування трактатів з чорної магії. Він був складений з видозмінених букв давньоєврейського алфавіту. Інший зберігся до пізніших часів: у 1775 році він був використаний у листі шпигуна, спрямованого регентові Алжиру [5: 120].

Досягнення арабів у галузі криптології були докладно викладені в праці Шехаба Калкашанді, що являє собою величезну 14-томну енциклопедію, написану в 1412 році для того, щоб подати систематичний огляд усіх важливих сфер криптологічних знань. Розділ під загальною назвою "Щодо приховування таємних повідомлень у літерах" містив дві частини: у першій ішлося про символічні дії та натяки, а друга була присвячена симпатичному чорнилу та криптології. Перший раз за всю історію шифрів в енциклопедії було репрезентовано список як систем перестановки, так і систем заміни. Більше того, у п'ятому пункті списку вперше згадувався шифр, для якого була характерна більше ніж одна заміна букв відкритого тексту; також розглядається перший в історії аналіз криптоаналітичного дослідження шифротексту.

Його джерела, очевидно, варто шукати в інтенсивному та скрупульозному вивченні Корану численними школами арабських граматиків. Поряд з іншими дослідженнями вони займалися підрахунком частотності вживання слів, намагаючись скласти хронологію розділів Корану, вивчали фонетику слів, щоб установити, чи були вони справді арабськими, або ж це – запозичення з інших мов. Важливу роль у виявленні лінгвістичних закономірностей, які призвели до виникнення арабського криптоаналізу, відіграв також розвиток лексикографії. Адже під час складання словників авторам фактично доводилося враховувати частоту вживаності літер, а також те, що букви, які ніколи не зустрічаються поряд, можуть знаходитися поруч одна біля одної. На той час частотний аналіз повідомлення дозволяв без зайвих зусиль розкривати шифри простої підстановки. На жаль, криптоаналітичні досягнення Калкашанді незабаром були забуті арабами [1; 5].

Цікаво, що в той час, коли прості люди шифрування вважали чаклунством, основні роботи у галузі криптографії та криптоаналізу виконувалися в межах католицької церкви. Так, в XIV столітті з'являється книга співробітника папської канцелярії Чікко Сімонетті, у якій він докладно викладає шифри заміни, в яких для вирівнювання частоти вживаності букв у шифротексті голосним буквам ставиться у відповідність не один знак, а декілька. Вперше зустрічається описання так званого шифру "лозунгу", що у різних модифікаціях буде застосовуватися навіть декілька століть потому. Правило заміни букв у ньому визначається в такий спосіб: під алфавітом пишеться ключова фраза-гасло, а вже потім букви, які в ньому не зустрічаються.

Майже через століття з'являється книга "Трактат про шифри", автор якої, Габріель де Лавінд, секретар папи Клементія XII, пропонує аналіз нового типу шифру, що допускає заміну букв декількома символами, кількість яких пропорційна частоті букв у відкритому тексті. Імена, посади, географічні назви рекомендується заміняти спеціальними знаками. Це був найдавніший зразок номенклатора – гібридної системи шифрування, яка у наступні 450 років поширилася по всій Європі.

У 1466 році знову ж таки в папській канцелярії з'являється трактат про шифри архітектора та філософа Леона Альберті, у якому пропонується спосіб приховування повідомлення в одному з нейтральних допоміжних текстів. Альберті пропонує свій власний шифр із назвою "шифр королів". По суті, Альберті винайшов багатоалфавітну заміну – новий вид шифрування, використовуваний у більшості сучасних шифросистем.

У 1518 році в Німеччині з'являється перша друкована книга з криптографії "Поліграфія". Її автор, абат Іоганнес Тритемій, розвиває ідею Альберті про багатоалфавітну заміну [1]. Алгоритм шифрування виглядає в такий спосіб: створюється таблиця заміни, першим рядком якої є власне саме повідомлення, другим – алфавіт, третім – алфавіт, зміщений на один крок і т. д. Під час шифрування перша буква повідомлення замінюється літерою, що знаходиться під нею у першому рядку, друга буква – літерою, що знаходиться в другому рядку і т. д.

На початку XVI століття Маттео Арженті, криптограф папської канцелярії, винайшов код, відповідно до якого можуть замінятися не тільки букви, але й склади, слова і навіть фрази. У цей же час з'являється й числовий код.

Наступним етапом розвитку криптографії можна вважати 1563 рік, коли у своїй книзі "Про таємну переписку" італійський натураліст Джованні Порта обгрунтував метод біграмного шифру, в якому здійснюється заміна не однієї букви, а пари букв. У своїй книзі Порта наводить приклади списків імовірних слів з різних галузей знань, істотно передбачивши те, що згодом криптологи назвуть "методом імовірного слова". Приблизно в той же час французький посол у Римі Блез Віженер, ознайомившись із працями з криптографії, пише книгу "Трактат про шифри" (1585), у якій він пропонує застосовувати відкритий або шифрований текст у якості ключа і висловлює думку про те, що "абсолютно все у світі являє собою шифр. Вся природа є просто шифром і секретним листом". Пізніше цієї думки дотримуватимуться Блез Паскаль і батько кібернетики Норберт Вінер.

Незабаром розвиток криптографії став давати плоди. Поразка Великої Армади в 1588 році у значній мірі була зумовлена умінням англійської криптографічної школи, яка без зусиль розкривала іспанські шифри і повідомляла про всі пересування ворожих сусідів. Криптографія була відома й застосовувалася в багатьох сферах суспільства Британії. Лондонець Самуель Пепіс (1633-1703) всесвітньо відомий своїм щоденником, за допомогою якого історики, використовуючи його як базис, пишуть праці про перехід від Пуританства до Реставрації. Мистецтвознавці включили цей доробок у світову скарбницю літератури. Пепіс закінчив Кембридж завдяки кузенові батька – адміралові Монтегю й мав багато друзів: ученого Ісаака Ньютона, архітектора Крістофера Рена, поета й драматурга Джона Драйдена. Пепіс був особисто свідком таких незабутніх для Англії подій, як повернення короля Чарльза II в Англію, чума 1664 року, пожежа Лондона 1666 року, революція 1688 року. Цікаво, що його мемуари були зашифровані згідно із системою криптолога Томаса Шелтона й додатково власним шифром, оскільки містили багато скандальних фактів про великих сучасників. Разом із його особистими книгами й паперами щоденник після смерті письменника потрапив у Кембридж, де відразу ж привернув увагу дослідників. Перший успіх у його розшифровці був отриманий лише в 1822 році, а повністю робота над ним завершилася у 1899 році.

Таким чином, до XVIII століття криптографія остаточно переросла у формат самостійної науки, здійснивши складний шлях розвитку та становлення. Однак історія тайнопису має ще багато нерозкритих секретів і, незважаючи на наявність професійних криптологів, які перебувають на державній службі, і постійного використання шифрів у дипломатії та військовій справі, криптологія вимагає подальшого дослідження, але вже на значно вищому рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Беляев Д., Гольчевский Ю. Введение в криптографию: Учебн. пособие. – Сыктывкар: Изд-во Сыктывкарского ун-та, 2004. – 152 с.
2. Винокуров А. Цикл статей по криптографии. Введение. 19 октября 1998.
3. Дориченко С., Ященко В. 25 этюдов о шифрах. – М.: ТЕИС, 1994. – 69 с.
4. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 335 с.
5. Кан Дэвид. Война кодов и шифров: История 4-х тысячелетий криптографии / Пер. с англ. Е. Алексеева. – М.: РИПОЛ Классик, 2004. – 528 с.
6. Лыгин Е. Тайнопись. Практическое пособие по ручному шифрованию. 2-е издание. – Саратов: Приволжское книжное изд-во, 1998. – 91 с.

Матеріал надійшов до редакції 15.04. 2009 р.

Мудрак Л. П. Из истории возникновения тайнописи.

В статье выяснена актуальность проблемы защиты информации и ее связь с разнообразными сферами человеческой деятельности. Исследовано историю возникновения криптографии и криптоанализа, рассмотрены способы шифровки давних цивилизаций. Приведены примеры использования шифровок в Библии. Очерчен вклад арабов в становление криптоанализа и роль католической церкви в последующей разработке и совершенствовании шифров.

Mudrak L. P. From the History of Cryptography Appearance.

In the article the topicality of information protection problem and its connection with the various spheres of human activity is found out. History of origin of cryptography and cryptanalysis is explored, the methods of enciphering of old civilizations are considered. The examples of the use of enciphering in Bible are given. The contribution of Arabs to becoming of cryptanalysis is outlined and the role of Catholic Church in subsequent development and perfection of codes.