ЗМІСТ

Історія криптології та секретного зв’язку

Про книгу

У виданні розповідається про історію народження й розвитку криптології та стеганографії, спеціальних видів засекреченого зв'язку у провідних країнах світу (СРСР, США, Великобританія, Німеччина), утворення їхніх криптологічних служб та апаратури засекречування, «шпіонську» діяльність спецслужб СРСР і США та їхню боротьбу у «полюванні» за шифрами супротивника, а також сучасний стан криптології у світі. Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет

ІСТОРІЯ КРИПТОЛОГІЇ ТА СЕКРЕТНОГО ЗВ'ЯЗКУ

Видавництво
«К Н Т»
Київ – 2023

УДК 004:056.52
І-89

Історія криптології та секретного зв'язку / упорядник Гребенніков В. В.
І - 8 9 — Київ: Вид. «КНТ», 2023. — 800 с.

ISBN 978-966-370-675-7

У виданні розповідається про історію народження й розвитку криптології та стеганографії, спеціальних видів засекреченого зв'язку у провідних країнах світу (СРСР, США, Великобританія, Німеччина), утворення їхніх криптологічних служб та апаратури засекречування, «шпіонську» діяльність спецслужб СРСР і США та їхню боротьбу у «полюванні» за шифрами супротивника, а також сучасний стан криптології у світі.

Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет.

УДК 004:056.52

ISBN 978-966-370-675-7

ЗМІСТ

«Хто володіє інформацією,
той володіє світом»
(Ротшильд)

Передмова

Майже чотири тисячі років тому в місті Менет-Хуфу на березі Нілу якийсь єгипетський переписувач намалював ієрогліфи, що розповіли історію життя його пана. Цей напис дійшов до наших днів та був вирізаний приблизно в 1900 році до н.е. на гробниці знатної людини на ім'я Хнумхотеп. Зробивши це, невідомий єгиптянин став родоначальником документально зафіксованої історії криптографії. Однак ці ієрогліфи все ж таки не були тайнописом у тому значенні, як його розуміють сьогодні. Для засекречування свого напису єгипетський переписувач не використав жодного повноцінного шифру, лише в окремих місцях намалював незвичайні ієрогліфічні символи замість більш звичних ієрогліфів.

Це свідчить про те, що вже з тих часів люди зрозуміли, що інформація становить визначену цінність та потребує захисту. В результаті її вирішили приховувати та почали робити це за допомогою доступних для свого часу способів. Спочатку писемність сама по собі була системою приховування інформації, тому що в давніх країнах нею володіли тільки обрані. Священні книги Давнього Єгипту та Давньої Індії тому приклади.

Поява писемності стала результатом потреби древньої людини виражати за допомогою символів божественні принципи. Форми цих символів (знаків) вона бачила в тріщинах каменів, на сніжному насті, у малюнках льоду… та вважала їх проявом божественної сили. Оскільки таким чином божество (або Природа) виражало свою волю, людина помічала ці символи та вважала їх священними.

Так, філософ Ф.Шеллінг писав: «Те, що ми називаємо природою, – лише поема, прихована в чудесному тайнописі». Такої ж думки і сучасний поет Ю.Мориць: «Тайнопис – почерк усієї світобудови, почерк поезії, кисті, клавіру! Тайнопис – це в тумані переказу вогненний шрифт сучасного світу».

Безперечно, найперші символи та знаки, написані чи видовбані в камені, або вирізані на дереві мали магічний характер. Найдавніші свідчення тому відносяться до 17-16 тисячоліття до н.е. На цих пам'ятниках писемності зображені фігури, що стали «прабатьками» відомих сьогодні магічних символів: хрестів, руней, колес, свастик. Згодом ці сакральні знаки накопичувалися, передавалися в одкровеннях, усно та до 3-1 тисячоліття до н.е. уже були системами, почали утворюватися перші магічні алфавіти.

Ці алфавіти осмислювалися в ті часи саме як набір священних символів із привласненими їм фонетичними значеннями, що дозволяло використовувати ці знаки для писемності. Так виникли родинні фінікійський, грецький, латинський, етруський і рунічний алфавіти, але досить значна частина древніх символів залишилася за межами цих алфавітів і продовжувала використовуватися винятково з магічною та художньою метою.

До нашого часу як магічний дійшов рунічний алфавіт. Руни (тобто знаки давньоскандинавського алфавіту) були розбиті на три групи по вісім штук у кожній. Основна система шифрування являла собою шифр заміни – кожній руні відповідали два знаки шифротекста (косі риски різної довжини). Число рисок зверху позначало номер групи, а знизу – номер руни в групі. Зустрічалися й ускладнення цієї системи, наприклад руни в групах перемішувалися.

До наших днів зберігся навіть пам'ятник давньої шведської криптографії – рекський камінь. Цей камінь висотою більше 4 метрів знаходиться на цвинтарі села Рьок. На ньому нанесено 770 зашифрованих руней.

Незважаючи на те, що пізніше в країнах Скандинавії стала застосовуватися латинська абетка, рунічне письмо використовувалося до XIX століття. Однак у XVI-XVIII століттях досить мало людей знало рунічні алфавіти, тому рунічний запис навіть без шифрування забезпечував збереження таємниці листування. Зокрема руни для захисту інформації використовував шведський генерал Якоб де ла Гарді під час тридцятирічної війни (1618–1646).

Готське слово «runa» означає «таємниця» і походить з древнього німецького кореня зі значенням «ховати». В сучасних мовах це слово також присутнє: німецьке «raunen» означає «нашіптувати», латиське «runat» – «говорити», фінське «*runo*» – «вірш, заклинання». Ще одним магічним алфавітом, який деякі автори відносять до «рунічних написів», є огамічний (*ogam, ogum, ogham*), розповсюджений в Ірландії, Шотландії, Уельсі та Корнуолі в III-X століттях н.е. У давньоірландських текстах було згадування про те, що «*ogam*» служив для

передачі таємних послань, а також для гадань.

Взагалі магічним алфавітом можна назвати будь-який алфавіт, тому що кожна буква кожного алфавіту має власне символічне значення. Особливо це стосується єврейського івриту та індійського санскриту, які поряд із грецьким і латинським алфавітами до цього часу використовуються окультистами. Однак, незважаючи на наявність сакральних значень у символів двох останніх, вони все-таки стали згодом, у першу чергу, ознаками вченості та культури тих, хто їх уживав.

Символізм, який був закладений у кожну букву, виконував дві функції: по-перше, він приховував таємниці від непосвячених, а по-друге, навпаки, відкривав їх тим, хто був цього гідний, хто розумів прихований зміст цих символів. Присвячені жреці вважали святотатством обговорення священних істин вищих світів або божественних одкровень вічної Природи на тій же мові, що використовувалася простим народом. Саме через це усіма сакральними традиціями світу розроблялися свої таємні алфавіти.

Іврит є одним із найпоширеніших алфавітів у Західній магічній традиції, а його букви вважаються умістищем божественної сили. Наприклад, буква єврейського алфавіту «алеф» означає владу, людину, мага; буква «бет» – науку, рот, двері храму; «гимель» – дію, протягнену для рукостискання руку тощо. В алхімії букви були також багатозначні: «*A*» виражало початок усіх речей; «*Y*» – відношення між чотирма основними елементами; «*L*» – розкладання; «*M*» – андрогінну природу води у її первісному стані тощо.

Грецький алфавіт, подібно івриту для євреїв, служив грекам одним із засобів пізнання світу. У греків букви «*A*», «*E*», «*H*», «*I*», «*O*», «*Y*» і «*Ω*» відповідали 7 планетам (небесам). Букви «*B*», «*Γ*», «*Δ*», «*Z*», «*K*», «*Λ*», «*M*», «*N*», «*Π*», «*P*», «*Σ*» і «*T*» приписувалися 12 знакам Зодіаку. Букви «*Θ*», «*Ξ*», «*Φ*» і «*X*» являли собою 4 світові елементи (стихії), а «*Ψ*» – «світовий дух». Алфавіт використовувався також для гадання та в різних містеріях. Так, наприклад, п'ята буква грецького алфавіту «*E*» (епсілон)

Α	α	альфа	Ν	ν	ню
Β	β	бета	Ξ	ξ	кси
Γ	γ	гамма	Ο	ο	омикрон
Δ	δ	дельта	Π	π	пи
Ε	ε	эпсилон	Ρ	ρ	ро
Ζ	ζ	дзета	Σ	σ	сигма
Η	η	эта	Τ	τ	тау
Θ	θ	тета	Υ	υ	ипсилон
Ι	ι	йота	Φ	φ	фи
Κ	κ	каппа	Χ	χ	хи
Λ	λ	лямбда	Ψ	ψ	пси
Μ	μ	мю	Ω	ω	омега

служила символом «Духовного Сонця» у великому храмі грецьких містерій у Дельфах, де протягом сімнадцяти століть проводилися елевсинські присвяти.

У латинському алфавіті голосні букви «*A*», «*E*», «*I*», «*O*», «*U*» і приголосні «*J*», «*V*» відповідали 7 планетам. Приголосні букви «*B*», «*C*», «*D*», «*F*», «*G*», «*L*», «*M*», «*N*», «*P*», «*S*» і «*T*» керували 12 астрологічними знаками. Букви «*K*», «*Q*», «*X*», «*Z*» відповідали 4 стихіям, а «H» являла собою «світовий дух». Латинський алфавіт використовувався в багатьох окультних значеннєвих фігурах.

У давніх цивілізаціях ми знаходимо два види письма: ієратичне, або священне письмо, що використовувалося священнослужителями для таємного спілкування один з одним, і демотичне письмо, що вживалося всіма іншими. Винахід першої системи скоропису, що споконвічно слугував як таємний лист, приписувався Туліусу Тиро, вільновідпущеному рабу Цицерона (106-43 роки до н.е.).

За свідченням Геродота в давньому Єгипті роль шифру відігравала спеціально створена жерцями мова. Там паралельно існували три алфавіти: письмовий, священний та загадковий. Перший з них відображав звичайну розмовну мову, другий міг використовуватися для викладу релігійних текстів, а третій застосовувався провісниками або для приховання змісту повідомлень. У давній Греції також існували десятки досить відмінних один від одного діалектів.

Діоген Лаертський так пояснював одну з причин вгасання філософії пифагорійців: «...записана вона була по-дорийські, а оскільки цей прислівник малозрозумілий, то здавалося, що й вчення, які на ньому викладають, не справжні й перекручені...». У книзі Е.Шюре «Великі присвячені» зустрічається фраза про те, що «з великою працею і великою ціною добув Платон один з манускриптів Піфагора, що ніколи не записував своє навчання інакше, як таємними знаками та під різними символами».

Фіванський алфавіт використовується й сьогодні завдяки старанням не тільки практиків середньовічних гримуарів, але й деяких містично налаштованих особистостей, що іменують себе «язичниками». Так само як і будь-який інший з категорії «магічних», фіванський алфавіт використовується для написання текстів заклинань та служить у таких випадках шифром (араб. *sifr* - ноль, ніщо, пустота).

Вчений Блез Паскаль писав: «Мови суть шифри, в яких не букви замінені буквами, а слова

словами, так що невідома мова є шифр, який легко розгадується». Так, мови американських індіанців неодноразово використовувалися як системи шифрування. Під час Першої світової війни індіанці племені «чокто (чахта)» були першими, хто допомагав Армії США шифрувати військові повідомлення, а на початку Другої світової війни для ВМС США це робили індіанці племені «навахо». У 1960 році ірландські збройні сили в Конго, направлені туди за рішенням ООН, здійснювали переговори на гельській мові.

З розвитком фонетичного письма писемність різко спростилася. У давньому семітському алфавіті у 2-му тисячолітті до н.е. було всього близько 30 знаків. Ними позначалися приголосні звуки, а також деякі голосні й склади. Спрощення письма стимулювало розвиток криптології та шифрувальної справи.

Правителям великих держав необхідно було здійснювати «приховане» керівництво намісниками в чисельних провінціях та одержувати від них інформацію про стан справ на місцях. Королі, королеви й полководці повинні були керувати своїми країнами та командувати своїми арміями, опираючись на надійний та ефективно діючий зв'язок. В результаті організація та забезпечення шифрованого зв'язку для них було життєво необхідною справою.

У той же час усі вони усвідомлювали наслідки того, що відбудеться, якщо їхні повідомлення потраплять не в ті руки, якщо ворожій державі стануть відомі важливі таємниці. І саме побоювання того, що вороги перехоплять повідомлення, послужило причиною активного розвитку кодів і шифрів – способів приховання змісту повідомлення таким чином, щоб прочитати його зміг тільки той, кому воно адресовано.

Прагнення забезпечити таємність означало, що в державах функціонували підрозділи, що створювали коди й шифри та відповідали за забезпечення таємності зв'язку шляхом розробки й використання самих надійних шифрів. А в цей же час дешифрувальники ворога намагалися розкрити ці шифри та видідати його таємниці.

Дешифрувальники являли собою алхіміків від лінгвістики, загін чаклунів, що намагалися за допомогою магії одержати осмислені слова з безглуздого набору символів. Історія кодів і шифрів – це багатовікова історія двобою між «творцями» та «зломщиками» шифрів, інтелектуальна гонка шифрувальної зброї, що вплинула на хід історії.

При написанні цієї книги я ставив перед собою чотири завдання. По-перше, викласти зібраний матеріал у хронологічній послідовності на українській мові, в чому і полягає новізна книги («фішка» - по молодіжній термінології). Історичні книги з питань криптології є тільки на російській та англійській мовах, тому я

вирішив виправити цей недолік. По-друге, доповнити історію криптології ще історією шифровально-документального та урядового телефонного зв'язку, оскільки для його функціонування також потрібні шифри. По-третє, показати еволюцію шифрів різних країн у хронологічній послідовності. Тут повною мірою підходить термін «еволюція», оскільки розвиток шифрів може розглядатися як еволюційна бо¬ротьба.

Шифр завжди є об'єктом атаки дешифрувальників. Як тільки дешифрувальники створюють новий засіб, що виявляє слабке місце шифру, подальше його використання стає безглуздим. Шифр або виходить із уживання, або на його основі розробляється новий, більш стійкий. У свою чергу, цей новий шифр використовується доти, поки дешифрувальники не знайдуть його слабке місце, і так далі.

Боротьба, що не припиняється між «творцями» та «зломщиками» шифрів, сприяла появі цілого ряду чудових наукових відкриттів. Шифрувальники постійно докладали зусиль для створення усе більш стійких шифрів щодо захисту систем і засобів зв'язку, у той час як дешифрувальники безупинно винаходили все більш потужні методи їхньої атаки.

У своїх зусиллях руйнування й збереження таємності обидві сторони залучали найрізноманітніші наукові дисципліни й методи: від математики до лінгвістики, від теорії інформації до квантової теорії. В результаті шифрувальники й дешифрувальники збагатили ці предмети, а їхня професійна діяльність прискорила науково-технічний прогрес, причому найбільш помітно це виявилося в розвитку сучасних комп'ютерів.

Роль шифрів в історії величезна. Шифри вирішували результати боїв і призводили до смерті королів і королев. Тому я звертався до історичних фактів політичних інтриг та розповідей про їхні життя й смерть, щоб проілюструвати ключові поворотні моменти в еволюційному розвитку шифрів. Історія шифрів настільки багата, що мені довелося опустити багато захоплюючих історій, що, у свою чергу, означає, що моя книга не занадто повна. Якщо ви захочете більше довідатися про розповіді, що вам сподобалися, або про дешифрувальника, що зробив на вас незабутнє враження, то я рекомендуювам звернутися до списку використаної літератури, що повинна допомогти тим читачам, які бажали б вивчити предмет більш детально.

Четверта мета книги полягає в тому, щоб показати, що шифри сьогодні мають набагато більше значення, ніж коли-небудь раніше. Оскільки інформація стає усе більше і більше цінним товаром, а революція у сфері комунікацій змінює суспільство, процес зашифровування повідомлень, або інакше, шиф-

рування, починає грати все більшу роль у повсякденному житті. Сьогодні наші телефонні розмови передаються по супутникових каналах, а наші електронні листи проходять через різні комп'ютери, і можна з легкістю здійснити перехоплення інформації, що ставить під загрозу наше приватне життя.

Шифрування – єдиний спосіб захистити наше приватне життя й гарантувати успішне функціонування електронного ринку. Мистецтво тайнопису, що перекладається грецькою як криптографія (гр. *kryptós* – таємний і *graphia* – пишу) дасть вам замки й ключі інформаційного століття. Щоб у подальшому вся викладена нижче інформація була зрозумілою, розглянемо основні поняття та терміни цієї науки.

Інформація, що може бути прочитана та зрозуміла без яких-небудь спеціальних заходів, називається відкритим текстом. Метод перекручування та приховування відкритого тексту таким чином, щоб сховати його суть, називається зашифруванням. Зашифрування відкритого тексту приводить до його перетворення у незрозумілу абракадабру, іменовану шифротекстом. Шифрування дозволяє сховати інформацію від тих, для кого вона не призначається, незважаючи на те, що вони можуть бачити сам шифротекст. Протилежний процес перетворення шифротексту в його вихідний вигляд називається розшифруванням.

Криптографія – це заходи щодо приховування та захисту інформації, а криптоаналіз (гр. *análysis* – розкладання) – це заходи щодо аналізу та розкриття зашифрованої інформації та криптографованих комунікацій. Разом криптографія та криптоаналіз створюють науку криптологію (гр. *lógos* – слово, знання).

Відкритий текст	Зашифрування	Шифр-текст	Процес передачі	Шифр-текст	Розшифрування	Відкритий текст

Криптологія – це наука про використання математики для зашифрування й розшифрування інформації. Криптологія дозволяє зберігати важливу інформацію при передачі її звичайними незахищеними каналами зв'язку (зокрема, Інтернет) у такому вигляді, що вона не може бути прочитаною або зрозумілою ніким, крім визначеного одержувача. Криптоаналіз являє собою суміш аналітики, математичних і статистичних розрахунків, а також спокою, рішучості та удачі. Криптоаналітиків також називають «зломщиками».

Криптографічна стійкість вимірюється тим, скільки знадобиться часу й ре-

сурсів, щоб із шифротексту відновити вихідний відкритий текст. Результатом стійкої криптографії є шифротекст , що надзвичайно складно «зламати» без володіння певними інструментами з дешифрування.

Криптографічний алгоритм, або шифр – це математична формула, що описує процеси зашифрування й розшифрування. Секретний елемент шифру, який повинен бути недоступним стороннім, називається ключем шифру.

Щоб зашифрувати відкритий текст або розмову, криптоалгоритм працює в поєднанні з ключем – словом, числом або фразою. Одне ж те саме повідомлення, зашифроване одним алгоритмом, але різними ключами, буде перетворювати його у різний шифротекст. Захищеність шифротексту цілком залежить від двох речей: стійкості криптоалгоритма та секретності ключа.

Найпростішим видом шифрування є кодування, де не використовується ключ. Хоча у сучасній криптології код не вважається шифром, однак він є таким – це шифр простої заміни. Кодування, як правило, містить у собі застосування великої таблиці або кодового словника, де перераховані числові відповідності (еквіваленти) не тільки для окремих букв, але й для цілих слів та найбільш використовуваних фраз і речень.

Отже, перейдемо до цікавої та захоплюючої історії криптології та спеціальних видів зв'язку...

Частина 1.

Історія європейської криптології

1.1. Поява шифрів

Взагалі всі шифри можуть бути розділені на два види: перестановка й заміна. При перестановці букви повідомлення просто переставляються, утворюючи анаграму. Для дуже короткого повідомлення, що складається, наприклад, з одного слова, такий спосіб досить ненадійний, оскільки існує вкрай обмежене число можливих способів перестановки жменьки букв. Так, 3 букви можуть бути розставлені всього лише 6 різними способами. Однак у міру збільшення чисельності букв кількість можливих перестановок стрімко зростає, і відновити вихідне повідомлення стає неможливо, якщо невідомий точний спосіб шифрування. Наприклад, якщо фраза складається з 35 букв, то кількість їхніх різних перестановок становить більше 50 000 000 000 000 000 000 000 000 000 000.

Якби одна людина змогла перевіряти одну перестановку в секунду, і якби всі люди на Землі працювали день і ніч, то, щоб перевірити всі можливі перестановки, треба було б часу в тисячі разів більше, ніж термін існування Всесвіту.

Створюється враження, що випадкова перестановка букв гарантує дуже високий ступінь безпеки, оскільки для супротивника дешифрувати навіть коротке речення виявиться нездійсненним. Однак при перестановці може утворитися неймовірно складна анаграма, і якщо букви випадково, ні з того ні із сього, переплутаються, то ні

одержувач, ні перехоплювач не зможуть її розшифрувати. Тому спосіб перестановки букв повинен бути заздалегідь обговорений відправником повідомлення і його одержувачем, але разом з тим зберігатися в таємниці від супротивника.

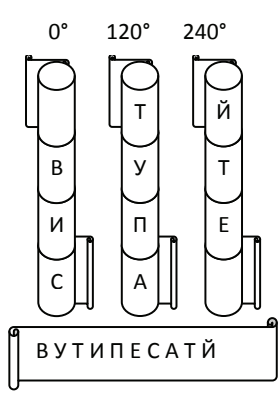
Першим шифрувальним пристроєм, який дійшов до нас та реалізовував шифр перестановки, була так звана «скитала» (scytale) або «сцитала» (близько VI-V ст. до н.е.), що використовувалась в античний період спартанцями.

Скитала являла собою дерев'яний циліндр, навколо якого намотувалася смужка шкіри або пергаменту. Відправник писав повідомлення по всій довжині скитали, а потім розмотував смужку, на якій після цього залишався безглуздий набір букв. Повідомлення виявлялося зашифрованим. Вісник брав шкіряну смужку й звичайно ховав повідомлення, використовуючи смужку як пояс, буквами усередину, тобто крім зашифровування застосовував також і стеганографію. Щоб одержати вихідне повідомлення, адресат просто намотував смужку шкіри навколо скитали того ж діаметра, що й скитала, якою користувався відправник.

У 404 році до н.е. до спартанського полководця Лісандра привели вісника, який був закривавлений та ледве тримався на ногах, одного з 5-ти вісників, що залишився живим після вкрай небезпечної подорожі з Персії. Вісник передав свій пояс Лісандру, що намотав його навколо своєї скитали й прочитав, що перський воєначальник Фарнабаз збирається напасти на нього. Завдяки скиталі Лісандр встиг підготуватися до нападу й відбив його.

Грецький історик Плутарх так описав цей спосіб шифрування:

«Відправляючи до місця служби начальника флоту або сухопутного війська, ефори вручають від'їжджаючому круглий ціпок. Інший, зовсім однакової довжини й товщини, залишають собі. Ці ціпки й називають скиталами. Коли ефорам потрібно повідомити яку-небудь важливу таємницю, вони вирізують довгу й вузьку, як ремінь, смугу папірусу, щільно, без проміжків намотують її на свою скиталу й пишуть на ній текст. Потім знімають смугу й без ціпка відправляють її воєначальнику. Оскільки букви на ній розміщують без усякого зв'язку, розкидані безладно, прочитати написане він може, тільки взявши свою скиталу й намотавши на неї вирізану смугу, щоб, водячи очами навколо ціпка й переходячи від попередньої до наступної, мати перед собою зв'язне повідомлення».



Це те ж саме, начебто букви писати не підряд, а через домовлене число по кільцю доти, поки весь

текст не закінчиться. Повідомлення «ВИСТУПАЙТЕ» при окружності палички в 3 букви дасть шифровку «ВУТИПЕСАТЙ».

Для прочитання шифровки потрібно було не тільки знати систему засекречування, але й мати ключ у вигляді палички визначеного діаметра. Знаючи тип шифру, але не маючи ключа, розшифрувати повідомлення було би складно. Шифр був досить популярний у Спарті й багато разів удосконалювався в пізніші часи. Про його важливе значення й велике поширення говорить свідчення Плутарха в «Порівняльних життєописах», коли історик повідомляє про життя грецького полководця Алкивіада: «Однак Лісандр звернув увагу на ці слова не раніше, ніж одержав з будинку скиталу з наказом відскіпатися від Алкивіада...»

Цей нехитрий спосіб часто використовувався через свою простоту та можливість оперативного розшифрування повідомлення. У той же час стійкість даного шифру була невелика, тому пізніше Архімед запропонував пристрій («антискитала»), за допомогою якого розшифровка подібного повідомлення без потрібного циліндра була досить простою та швидкою. Ремінь намотували на конічний «спис» і зрушували нагору й униз доти, поки не знаходили потрібний діаметр і текст повідомлення ставав зрозумілим.

Альтернативним шифру перестановки був шифр заміни, у якому кожна буква у вихідному тексті замінялася іншою буквою. Один з перших описів шифру заміни був приведений у «Камасутрі», тексті, написаному в 4-му столітті н.е. священиком-браміном Ватсьяяною, але заснованому на манускриптах, що відносяться до 4-го століття до н.е.

Згідно з «Камасутрою», жінки повинні опанувати 64 мистецтва, такі як готування їжі й напоїв, мистецтво одягання, масажу, готування ароматів. У цей список також входили менш очевидні мистецтва: чаклунство, гра в шахи, палітурна справа й теслярство. Під номером 45 у списку знаходилося мистецтво тайнопису *«mlecchita-vikalpa»*, призначене для того, щоб допомогти жінкам приховати подробиці своїх любовних зв'язків.

Один із рекомендованих способів полягав у тому, щоб розташувати попарно букви алфавіту випадковим чином, а потім заміняти кожну букву у вихідному повідомленні її парною (симетричною). Якщо застосуємо цей принцип до латинського алфавіту, то можемо скласти таку таблицю (лінійку) шифрування:

D	A	M	H	I	K	O	Z	R	S	U	W	Y
X	B	T	V	G	J	C	L	N	E	Q	F	P

Тоді замість слова «*UKRAINE*» відправник напише слово «*QJNBGRS*»**.**

На Близькому Сході один з перших шифрів заміни був розроблений древніми євреями та називався «темура» – «обмін». 22 букви єврейського алфавіту ділилися на дві частини, причому одна містилася над іншою; потім верхні букви замінялися

на нижні або навпаки. Можна було встановити всілякі комбінації залежно від місця поділу алфавіту й напрямку переміщуваних букв.

Найпростіший спосіб полягав у поділі алфавіту посередині так, щоб перші дві букви, «А» і «Б», збігалися із двома останніми, «Т» і «Ш». Ці букви й дали назву методу шифрування – «Атбаш» (англ. *Atbash*). Це був простий шифр одноалфавітної заміни для єврейського алфавіту. Таблиця (лінійка) шифрування цим методом для латинського алфавіту буде виглядати таким чином:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Бачимо, що у цьому шифрі заміна має симетричний вигляд. Так, наприклад, слово «*UZHGOROD*» перетворювалося у слово «*FASTLILW*».

Інший шифр «Альбам» полягав у розбивці алфавіту на дві частини та розташуванні однієї частини під іншою:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Слово «UZHGOROD» перетворювалося вже у слово «HMUTBEBQ».

Перше документально підтверджене використання шифру заміни у військових цілях з'явилося у «Записках про галльську війну» (лат. *Commentarii de Bello Gallico*) Гая Юлія Цезаря (I століття до н.е.). Цезар описував, як він послав повідомлення Цицерону, що перебував в облозі та був на грані капітуляції. У цьому листі латинські букви були замінені грецькими, тому ворог його не зміг би зрозуміти.


C. IVLII
CÆSARIS
COMMENTARII
DE BELLO GALLICO
ET CIVILI
TOMUS I.
VENETIIS MDCCLXXXIII

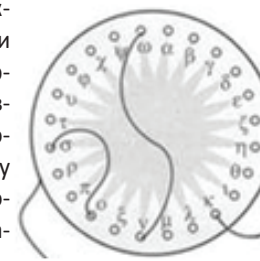
Цезар так часто користувався тайнописом, що Марко Валерій Проб написав цілий трактат про застосовувані ним шифри, який, на жаль, не дійшов до наших днів. Однак завдяки твору Гая Транквілла Светонія «Життя 12 Цезарів», написаному в 2-му столітті н.е., у нас є докладний опис одного з шифрів заміни, що застосовувалися Юлієм Цезарем. Він просто заміняв кожну букву в посланні буквою, що знаходилась в алфавіті на три позиції далі.

Ось як про це повідомляє Гай Светоній: «Існують і його листи Цицерону та листи до близьких про домашні справи: у них, якщо потрібно було повідомити що-небудь негласно, він користувався тайнописом, тобто міняв букви так, щоб з них не складалося жодного слова. Щоб розібрати й прочитати їх, потрібно читати щоразу четверту букву замість першої».

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Спочатку виписувався алфавіт у природному порядку, а потім під ним виписувався той же алфавіт, але зі зрушенням на 3 букви вліво. При зашифруванні буква «*A*» замінялася буквою «*D*», «*B*» замінялася на «*E*», «*C*» – на «*F*» й так далі. Так, наприклад, слово «*UZHGOROD*» перетворювалося у слово «*XCKJRURG*», а «*UKRAINE*» – у «*XNUDLQH*». Одержувач зашифрованого повідомлення шукав ці букви в нижньому рядку та по буквах над ними відновлював вихідне слово. Ключем у шифрі Цезаря була величина зрушення нижнього рядка алфавіту, тобто цифра 3. Спадкоємець Юлія Цезаря – Цезар Август – використовував той же шифр, але з ключем зрушення 4.

Вже у IV столітті до н.е. робилися спроби «механізації» криптологічної справи, пов'язані насамперед з ім'ям давньогрецького полководця Енея Тактики, захисника Трої, друга Гектора. Він створив так званий «диск Енея», що одержав у Давній Греції широке застосування. У диску діаметром 10-15 см і товщиною 1-2 см висвердлювалися отвори, що відповідали буквам алфавіту, через які просмикувалася нитка відповідно до букв шифрованого тексту. Для розшифрування нитку витягали, одержуючи зворотню послідовність букв. Цей примітивний на перший погляд спосіб шифрування був досить ефективний, тому що супротивнику, який перехопив повідомлення, було невідомо, яка буква відповідає кожному отвору. Крім того, якщо виникала небезпека перехоплення повідомлення, нитку можна було легко порвати, тим самим знищивши його.



Ідея Енея була використана при створенні й інших оригінальних шифрів заміни. Зокрема, в одному з варіантів замість диска використовувалася лінійка з кількістю отворів, рівних кількості букв алфавіту. Кожний отвір позначався своєю буквою, а букви по отворах розташовувалися в довільному порядку. До лінійки була прикріплена котушка з намотаною на неї ниткою. Поруч із котушкою був проріз. При шифруванні нитка простягалася через проріз, а потім через отвір, що відповідав першій букві шифрованого тексту, при цьому на нитці зав'язувався вузлик у місці проходження її через отвір. Потім нитка поверталася в проріз й

аналогічно зашифровувалася друга буква тексту й т.д. Після закінчення шифрування нитка витягалася й передавалася одержувачу повідомлення. Той, маючи ідентичну лінійку, простягав нитку через проріз до отворів, обумовлених вузлами, і відновлював вихідний текст по буквах отворів.

Цей пристрій одержав назву «лінійка Енея». Шифр, реалізований лінійкою Енея, був одним з прикладів шифру заміни: коли букви замінялися на відстані між вузликами з урахуванням проходження через проріз. Ключем шифру був порядок розташування букв по отворах у лінійці. Супротивник, що одержав нитку (навіть, маючи лінійку, але без нанесених на ній букв), не міг прочитати передане повідомлення. Аналогічне «лінійці Енея» «вузелкове письмо» отримало поширення в індіанців Центральної Америки. Свої повідомлення вони також передавали у вигляді нитки, на якій зав'язувалися різнобарвні вузлики, що визначали зміст повідомлення.

Ще один винахід стародавніх греків – так званий «квадрат Полібія». Грецький письменник Полібій (біля 200 – 120 до н.е.) використовував систему сигналізації, що була широко прийнята як метод шифрування. Він записував букви грецького алфавіту в квадратну таблицю та заміняв їх числовими координатами в таблиці номером рядка та номером стовпця. Пари чисел передавалися за допомогою смолоскипів. У варіанті з латинським алфавітом для передачі, наприклад, букви «U» потрібно було взяти 4 смолоскипи в праву руку та 5 – у ліву, або записати як цифру «45».

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Наприклад, слово «*UKRAINE*» можна записати як цифровий шифротекст «45254211243315» або «54522411423351».

Цікаво, що шифр Полібія дійшов до наших днів та одержав своєрідну назву «шифру в'язнів». Для його використання потрібно було тільки знати природний порядок розташування букв алфавіту (як у вищезазначеному прикладі для англійської мови). Число 3, наприклад, передавалося шляхом потрійного стукоту. При передачі букви спочатку відстукувалося число номера рядка, у якому знаходилася буква, а потім число номера відповідного стовпця. Наприклад, буква «F» передавалася подвійним стукотом (другий рядок) і потім одинарним (перший стовпець).

Із застосуванням цього шифру пов'язані деякі історичні казуси. Так, росій-

ські «*декабристы*», які були ув'язнені після невдалого повстання, не змогли встановити зв'язок з князем Одоєвським. Виявилося, що він (добре освічений за тих часів) не пам'ятав природний порядок розташування букв у російському та французькому алфавітах (іншими мовами він не володів). «Декабристи» для російського алфавіту використовували прямокутник розміру 5х6 (5 рядків та 6 стовпців) і скорочений до 30 букв алфавіт.

Пізніше букви стали розташовувати в квадраті хаотично, але це вимагало наявність такого квадрата у отримувача повідомлення, що також було небезпечно. Вихід був знайдений у застосуванні так званого ключового слова, що легко запам'ятовувалося. Обиралося недовге слово (наприклад, «UKRAINE»), з нього забиралися букви, що повторювалтся, а ті, що залишалися, записувалися в перші клітини квадрата по рядках. Порожні клітини заповнювалися буквами алфавіту, що залишилися, у природному порядку.

	1	**2**	**3**	**4**	**5**
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

В результаті такого шифрування слово «*UZHGOROD*» перетворюється у цифровий шифротекст «11553332414125».

Полібійський квадрат став однією з найбільш широко розповсюджених криптосистем, що вживалися у той час. Цьому сприяла його досить висока стійкість (у всякому разі, до автоматизації дешифрувальних систем): квадрат 5х5 для латинського алфавіту містить 155112100433310000000000000 (розрахунок досить приблизний) можливих положень, що практично виключає його дешифрування без знання ключа.

Ледащі й тому винахідливі римляни в IV столітті до н.е., щоб спростити процедуру шифрування, почали застосовувати два шифрувальні диски. Кожний із дисків, розміщених на загальної вісі, містив на своєму ободі алфавіт у випадковій послідовності. Кожній букві першого диска відповідала буква другого, що й становило шифр. Знайшовши на одному диску букву тексту, з іншого диска зчитували відповідну їй букву шифру. Такі прилади, що породжували шифр простої заміни, використовувалися аж до епохи Відродження.

Ці криптосистеми активно застосовувалися в Давній Греції та Римі й надовго визначили характер криптології. В умовах потреби ручного розшифрування, по-

лібійський квадрат був практично невразливим шифром, а скитала та диск Енея були досить прості, проте дозволяли оперативно зашифровувати й розшифровувати інформацію, що робило їх вигідними, скажімо, в польових умовах для оперативної передачі наказів.

Із занепадом античної цивілізації та утворенням у Європі варварських держав, криптологія занепала. Велика шкода її розвитку була завдана в часи середньовічної інквізиції. Всі кращі досягнення цивілізації, а разом з ними й криптологія, були втрачені. За свідченням святого Джерома «увесь світ поринув у руїни». В умовах, коли грамотність була вкрай низька, зашифровувати повідомлення не було необхідності, тому й самих письмових повідомлень практично не було.

Так, король франків Карл Великий, заснувавший у 800 році Священну Римську імперію, навчився читати й писати тільки у 50 років. Проте Карл Великий знав і використовував у листуванні зі своїми генералами шифр заміни букв алфавіту групою символів.

Освіта й грамотність у ті часи зосередилися в церкві, тому тайнопис став її монополією. Церква ухвалила, що простим парафіянам не можна приховувати таємниці від «Господа», а тайнопис – це «єресь». За використання тайнопису передбачалися жорстокі заходи покарання, аж до страти.

Крім вищеперерахованих причин, криптологія перебувала в занепаді ще й тому, що в ній бачили елементи чаклунства. Набір незрозумілих букв або символів, сам по собі схожий на заклинання, сприймався як щось магічне, а люди, що розуміли у цьому наборі символів зміст, розцінювалися як чаклуни або ворожки, що не могло не накласти свій відбиток на ставлення до них у християнській Європі.

З перших днів свого існування криптологія мала на меті сховати зміст важливих розділів письмових документів, що мали відношення до таких сфер магії, як гадання й заклинання. В одному з рукописів про магію, що датується III століттям н.е., був використаний шифр, щоб сховати важливі частини чаклунських рецептів. Криптографія часто була на службі магії в часи середньовіччя, і навіть в епоху Відродження за допомогою шифрів алхіміки засекречували важливі частини формул одержання «філософського каменя».

До шифрування інформації «призивалися» містичні сили. Так, наприклад, рекомендувалося використовувати «магічні квадрати». У квадрат розміром 4 х 4 вписувалися числа від 1 до 16. Його магія полягала в тому, що сума чисел по