<u>Лекція №1 (НЕ 1.1, 2 год.)</u>. Короткий історичний нарис. Основні поняття та визначення криптології.

План лекції:

1. Вступ.
2. Основні поняття та визначення криптології.
3. Короткий історичний нарис розвитку криптології.

Зміст лекції.

1. Вступ.

Задача захисту інформації в комп‘ютерних системах перетворюється сьогодні в одну з найактуальніших внаслідок широкої розповсюдженості таких систем, а також розширення локальних і глобальних комп‘ютерних мереж, якими передаються величезні об‘єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення сторонніх осіб з цією інформацією.

Не менш важливою задачею вважається широке впровадження в різні сфери діяльності людини електронного документообігу, який повинен забезпечуватися юридичною чинністю підписаних електронних документів.

Усі ці та багато інших задач захисту інформації покликана вирішувати криптографія.

Криптографічні механізми настільки тісно пов'язані з сучасними інформаційними технологіями, що разом з підвищенням комп'ютерної грамотності необхідно опановувати основи криптографії.

Грецьке слово *cryptos* перекладається як «таємниця», а отже, криптографія означає тайнопис. Звідси випливає, що початковим завданням криптографії було розроблення методів, спрямованих на приховування змісту переданої або збереженої інформації. І хоча на цей час сфера застосування криптографічних механізмів значно розширилася, основні ідеї можна проілюструвати саме на прикладі забезпечення конфіденційності інформації.

2. Основні поняття та визначення криптології.

Існує безліч публікацій, які містять історичні огляди з криптографії. Відзначимо лише, що кожному етапові розвитку цивілізації властиві відповідні криптографічні пристрої. Тривалий час шифрування текстів виконувалося вручну. Їх створення можна було вважати скоріше мистецтвом, ніж якоюсь стандартною процедурою. Відомо два протилежні погляди щодо шифрів. Відповідно до першого можна створити шифр, який неможливо розкрити. Другий погляд відбивав таку точку зору: малоймовірно, що «загадку», яка лежить в основі створеного шифру, не можна розгадати. Згодом ***науку про перетворення інформації у незрозумілу для сторонніх осіб форму*** стали називати ***криптографією***. Методи пошуку «розгадки» стали називати *криптоаналітичними методами,* а відповідну галузь досліджень — *криптоаналізом.* Отже, ***криптоаналіз – це наука, спрямована на подолання криптографічного захисту***. Тепер усе ширше використовують термін ***криптологія****,* тобто наука про шифри. Вважають, що криптологію складають дві великі частини, які доповнюють одна одну, — ***криптографія*** та ***криптоаналіз***.

Процес криптографічного перетворення інформації ми будемо називати ***шифруванням*** (або ***зашифруванням***, як це часто використовується у криптологічній літературі). Зашифровану інформацію повинні прочитати ті особи, для кого призначена ця інформація. Перш, ніж прочитати, її треба перетворити у зрозумілу форму. Цей процес, який ми будемо називати ***розшифруванням***, виконується за допомогою деякої секретної частини криптографічної системи – ***криптографічного ключа*** (або просто ***ключа***).

Супротивник, який перехопив зашифровану інформацію, як правило, не має такого ключа. Тому він намагається подолати криптографічний захист за допомогою криптоаналітичних методів. Такий спосіб, тобто розшифрування повідомлення без знання

ключа, ми будемо називати ***дешифруванням***. Отже, можна сказати, що розшифровують «свої», а дешифрують – «чужі».

Методи криптографічного захисту інформації можуть реалізовуватися як апаратно, так і програмно. Апаратна реалізація має суттєво більшу вартість, однак водночас, і більшу продуктивність та захищеність. Програмна реалізація практичніше, дешевша та гнучкіша у використанні.

3. Короткий історичний нарис розвитку криптології.

Проблема захисту інформації шляхом перетворення її у незрозумілу для сторонніх осіб форму хвилювала людство дуже давно. Історія криптографії налічує не менше років, ніж історія людської мови. Більше того, сама письмова мова була своєрідною криптографічною системою, оскільки нею на ранніх етапах розвитку людства володіли одиниці. Отже історія криптографії має вже не менше трьох тисяч років.

Прийнято вважати, що вона складається з чотирьох великих етапів:

1. Наївна криптографія (до початку XVI сторіччя);
2. Формальна криптографія (поч. XVI сторіччя – поч. XX ст.);
3. Наукова криптографія (30-60 рр. XX ст.);
4. Комп‘ютерна криптографія (60 рр. XX ст. – теперішній час).

Для ***наївної криптографії*** характерним є використання будь яких методів прихову-вання інформації, зокрема *кодування* та *стеганографія*.

Серед криптографічних методів використовувалися *перестановки* та *моноалфавітні підстановки* (заміни). *Шифрами перестановки* називають перетворення, які призводять лише до зміни порядку слідування літер у відкритому тексті. *Шифрами заміни* будемо називати такі перетворення, коли кожна літера вхідного тексту замінюється іншими символами, причому порядок слідування символів у повідомленні не змінюється.

Одним з перших зафіксованих прикладів використання шифрів є т. зв. шифр «сцитала» спартанського царя Лісандра. Цей шифр відомо з часів війни Спарти проти Афін у V ст. до н.е. Для його реалізації використовувалась т.зв. „сцитала” – циліндричний жезл певного діаметру. На сциталу намотували вузьку папірусну стрічку і на ній писали повідомлення вздовж осі сцитали. Коли стрічку знімали, на ній залишалися незрозумілі літери. Для розшифровки повідомлення адресат намотував стрічку на такий самий жезл і читав повідомлення.

Найстаршим шифром підстановки вважається шифр Цезаря, коли кожна літера вихідного тексту замінюється іншою літерою тої ж абетки, третю справа від неї. Іншим прикладом моноалфавітної підстановки є «магічний квадрат», авторство якого приписують грецькому письменнику Полібію. Детальніше про ці та інші алгоритми шифрування дивись далі.

Етап ***формальної криптографії*** (поч. XVI сторіччя – поч. XX ст.) звичайно пов‘язують з появою формалізованих алгоритмів, досить стійких для криптоаналізу вручну. В європейських країнах це сталося в період Відродження, коли розвиток науки і торгівлі потребували надійних способів захисту інформації. На цьому етапі активно використовуються т.зв. матричні шифри, перестановки в яких задаються одним або двома ключовими словами (див. далі). Важлива роль на цьому етапі належить Леонові Баптисті Альберті, італійському архітектору, який одним з перших запропонував багатоалфавітну підстановку. Цей шифр пізніше отримав назву французького дипломата XVI сторіччя Блеза Віженера. Метод шифрування полягав у послідовному «додаванні» літер відкритого тексту з ключовим словом. Цю процедуру можна полегшити використанням спеціальної таблиці, таблиці Віженера. Лише в 60-х роках XIX ст. офіцер прусських військ Касіскі виявив, що цей шифр можна частотно аналізувати.

Однією з перших наукових робіт, де сформульовано та узагальнено існуючі на той момент алгоритми шифрування, є «Поліграфія» (1508 рік) німецького абата Йоганна

Тритеміуса. Йому належать два невеликих але важливих відкриття: спосіб заповнення полібіанського квадрату за допомогою ключової фрази та шифрування пар літер (біграм).

Простим та ефективним способом багатоалфавітної заміни (шифрування біграм) є шифр Play-fair (його ще іноді називають шифром Плейфера), який було запропоновано Чарльзом Уітстоном на початку XIX ст. Цей шифр застосовувався аж до Першої світової війни, оскільки погано піддавався криптоаналізу вручну.

У XIX ст. голландець Аугуст Керкхоффс сформулював головне правило сучасної криптографії: ***секретність криптосистеми повинна визначатися не секретністю алгоритму, а секретністю ключа***.

У роки Першої світової війни з'явилися подрібнювальні шифри, найвідомішим представником яких був шифр ADGVX, який використовувався німецькою армією. Шифр ADGVX був поєднанням перестановок і підстановок. Цей алгоритм було розкрито французьким криптоаналітиком Жоржем Пенвеном.

1917 рік було ознаменовано появою багатообіцяючого шифру одноразового блокноту. Його розробили інженери фірми AT&T Г. Вернам та Дж. Моборн і використовували для захисту телетайпного зв'язку. Цей шифр можна вважати узагальненням шифру Віженера на випадок, коли довжина ключа збігається з довжиною повідомлення. Шифр одноразового блокноту абсолютно надійний, однак незручний у використанні. Назва шифру походить від того, що агент, який використовував цей шифр, після кожного сеансу зв'язку знищував сторінку шифроблокноту з ключем, на якому виконував шифрування поточного повідомлення.

Найвищим етапом розвитку формальної криптографії були *роторні шифрувальні машини*. Використання таких машин значно ускладнило, а з їх вдосконаленням і унеможливило ручний криптоаналіз. Однією з перших подібних систем була винайдена майбутнім президентом США Томасом Джеферсоном у 1790 році механічна роторна машина.

Попередником сучасних роторних шифрувальних пристроїв була машина, винайдена у 1917 році Едвардом Хепберном з Окленда, штат Каліфорнія. Цими машинами користувалася уся військова криптографія на протязі приблизно 50 років. Базовими елементами роторної машини є сам ротор та механічне колесо, яке служить для виконання операції підстановки.

У початковому варіанті роторна машина мала клавіатуру та чотири колеса, які оберталися на одній осі. На кожному колесі з лівого і правого боків було по 25 електричних контактів, що відповідали 25 літерам латинської абетки (літери I та J ототожнили). Контакти з лівого і правого боку було попарно з'єднано всередині колеса в певному порядку. Наприклад, ротор можна використовувати для заміни A на L; B на U; C на Z і т.д. Під час роботи машини колеса складалися разом, і їх контакти, доторкаючись один до одного, забезпечували проходження електричного сигналу через усі чотири колеса. Наприклад (Ємець), у чотирироторній машині перший ротор міг замінювати A на L, другий - L на V, третій – V на D; четвертий – D на S. Літера S і є остаточним результатом шифрування відкритого тексту. При натисканні літер на клавіатурі ротори проверталися подібно до електролічильника, забезпечуючи таким чином величезний період таблиці замін.

Найвідомішою роторною шифрувальною машиною, звичайно, була німецька *Енігма* (в перекладі – *загадка*), яка була сконструйована Артуром Шербіусом. *Енігма* складалася з батареї, щоби не залежати від джерела живлення, групи роторів (від трьох до п'яти), які можна було замінювати, та комутаційної панелі, за допомогою якої вхідний текст піддавали перестановкам.

Перед роботою машину треба було налаштувати. Налаштування зводилося до встановлення потрібної групи роторів у певному порядку, який визначався статичним ключем (наприклад, 5-3-4-1-2). Ротори провертали один відносно одного так, щоби у віконці на передній панелі пристрою утворилося кодове слово і приводили у контакт.

Після цього з‘єднували потрібні контакти комутаційної панелі для первісного перемішування вхідного тексту. Спосіб з‘єднання задавався ще одним статичним ключем. Далі необхідно було встановити ротори у певне початкове положення та перевірити правильність налаштувань, для чого на клавіатурі набирали контрольний текст (який також можна вважати своєрідним ключем) та слідкували, щоби отримати на виході системи контрольний зашифрований (або розшифрований) текст. Тепер машина готова до роботи. Працювали на цій машині два шифрувальники. Один набирав на клавіатурі відкритий текст (або шифротекст), а другий записував на папері літери, які висвічувалися на передній панелі пристрою.

Роторні машини активно використовувалися не лише німецькою армією. Відомі аналогічні апарати *Sigaba* (США), *Typex* (Велика Британія), Red, Orange, Purple (Японія). Роторні шифрувальні системи – вершина формальної криптографії, оскільки відносно просто реалізовували дуже стійкі, як на той час, шифри. Успішні криптоатаки на роторні машини стали можливими лише з винаходом перших комп‘ютерів у 40-х роках XX сторіччя.

Етап ***наукової криптографії*** характеризується появою криптосистем з математично обґрунтованою криптостійкістю. До початку 30-х років XX ст. остаточно сформувалися такі розділи математики, як теорія ймовірностей та математична статистика, загальна алгебра, теорія чисел; почали активно розвиватися теорія алгоритмів, теорія інформації та кібернетика.

Епохальною в цьому розумінні стала робота ***Клода Шеннона «Теорія зв‘язку в секретних системах»*** (1949 р.) де сформульовано основні теоретичні принципи криптографічного захисту інформації. К.Шеннон увів поняття «розсіювання», «перемішування», надмірності мови, обґрунтував можливість створення як завгодно стійких криптосистем. Матеріал статті, первісно був викладений у таємній доповіді «Математична теорія криптографії» (1945 р.), яку було розсекречено після закінчення Другої світової війни.

Стаття розділена на три частини (К.Шеннон). У першій частині наведено математичні основи побудови секретних систем. Секретну систему визначено абстрактно, як деяку множину відображень одного простору (множина можливих повідомлень) в інший (множину можливих шифрограм). Кожне конкретне відображення з цієї множини відповідає способу шифрування за допомогою конкретного криптографічного ключа. З кожною мовою пов‘язаний деякий параметр, який К.Шеннон назвав надмірністю мови. Надмірність вимірює наскільки можна скоротити певне повідомлення без втрати будь якої частини інформації. Надмірність мови грає центральну роль у криптології. Зокрема саме надмірність мови дозволяє використовувати для розкриття шифрів принципи частотного криптоаналізу.

У другій частині статті розглянуто проблему теоретичної секретності, а саме наскільки легко конкретна криптосистема піддається розкриттю за умови, що для аналізу перехоплених шифрограм супротивник має необмежені часові та матеріальні ресурси. «Ідеальну секретність» К.Шеннон визначає такими вимогами до системи. Вимагається, щоби апостеріорні ймовірності різних повідомлень, отримані після перехоплення супротивником певної шифрограми, точно дорівнювали апріорним ймовірностям тих же повідомлень до перехоплення. Ідеальний шифр, за твердженням К.Шеннона, існує однак вимагає у випадку кінцевої кількості повідомлень такої самої кількості ключів. При цьому довжина ключа повинна дорівнювати довжині повідомлення. Крім того, кожний ключ повинен використовуватися лише один раз. У цьому ж розділі К.Шеннон вводить поняття «інтервал єдиності», тобто мінімальної довжини шифрограми, за якої можливе однозначне за змістом її дешифрування.

Третя частина присвячена «практичній секретності». Дві криптосистеми з однаковою довжиною ключа можуть бути розв‘язані єдиним чином, однак значно відрізняються необхідними для цього часовими та матеріальними ресурсами. На основі

аналізу недоліків алгоритмів пропонуються методи побудови систем, для розкриття яких потрібні великі часові та матеріальні витрати. Також розглядається проблема несумісності різних вимог до криптосистем.

У 60-х роках XX ст. провідні криптографічні школи впритул підійшли до створення *блочних шифрів*, ще стійкіших за роторні машини, однак їх практична реалізація стала можливою лише за допомогою комп'ютерної техніки.

Комп'ютерна криптографія стала можливою з появою потужних і компактних обчислювальних пристроїв, використання яких надало можливість розробки блочних шифрів. Одним з перших був американський стандарт шифрування DES (його було прийнято 23 листопада 1976 р.). Один з його авторів, Хорст Фейстель з IBM розробив алгоритм, призначений для апаратної реалізації (т.зв. *сітка Фейстеля*). Характерні риси: обробка за один цикл лише половини блока тексту; робота з бітами, а не з байтами інформації (що сповільнює комп'ютерну реалізацію); можливість використання одного набору мікросхем як для зашифрування, так і для розшифрування повідомлень. Первісний алгоритм під назвою *Люцифер*, розроблений математиками фірми IBM на чолі з Х.Фейстелем, був поданий до Агентства національної безпеки США для аналізу. АНБ, модифікувавши статичні ключі алгоритму, скоротило ключ шифрування з 128 до 64 біт (8 з яких використовувалися як біти парності, так що секретна частина ключа складала усього 56 біт). Такий модифікований алгоритм і було прийнято в якості стандарту шифрування DES. При цьому, як це слідує з повідомлень у пресі, АНБ недооцінило темпи розвитку комп'ютерної техніки, що призвело до надто швидкого «старіння» алгоритму. Вже на початку 90-х років стало можливим організувати атаку прямого перебору ключів за допомогою розподілених обчислень. Таким чином, алгоритм вже не міг використовуватися в якості стандарту шифрування США. АНБ оголосило всесвітній конкурс криптографічних алгоритмів на звання нового стандарту шифрування. У 2001 році в якості нового стандарту, який отримав назву AES, було прийнято алгоритм Rijndael бельгійських криптографів Вінсента Ріймена та Джоана Даймена. Цей алгоритм не використовує сітку Фейстеля, а побудований на групі еліптичної кривої над кінцевим полем Галуа. Увесь блок вхідного тексту повністю обробляється за один цикл. Крім того, AES працює зі змінною довжиною блоку та ключа, що дає можливість зміни криптостійкості в залежності від ступеня секретності інформації.

Стандарт DES був не єдиним алгоритмом, який використовував сітку Фейстеля. Одним з найбільш стійких таких алгоритмів є ГОСТ 28147-89. Його було прийнято в якості стандарту шифрування СРСР у 1989 році. При проектуванні цього алгоритму криптографи КДБ узагальнили досвід десятирічного використання DES, значно збільшивши криптостійкість за допомогою використання 32 циклів шифрування та 256-бітного ключа. Це дало змогу спростити раундову функцію та процедуру розгортання ключа. Необхідно сказати, що нам досі не відомо повідомлень про успішний криптоаналіз ГОСТ 28147-89. Алгоритм й зараз використовується для захисту інформації в Росії та Україні, в тому числі для інформації з найвищим ступенем секретності.

У 1976 році сталася ще одна видатна подія в галузі криптографії: було розроблено основні принципи *асиметричної криптографії*. Започаткувала це робота Уітфілда Діффі та Мартіна Хеллмана «Нові напрямки сучасної криптографії». Тут вперше сформульована можливість обміну зашифрованими повідомленнями без обміну секретними ключами шифрування. Кількома роками пізніше Рональд Рівест, Аді Шамір та Леонард Аделман розробили асиметричну криптосистему RSA (названа по перших літерах прізвищ авторів), крипостійкість якої ґрунтується на складності розкладання великого числа на прості множники. Асиметрична криптографія, крім вирішення проблеми розповсюдження ключів, основної слабості симетричних криптосистем, відкрила одразу кілька нових прикладних напрямків, зокрема системи *електронного цифрового підпису* та *електронних грошей*.

У 80-90 роках XX сторіччя розробляються абсолютно нові революційні ідеї в області криптографічного захисту інформації: квантова криптографія та імовірнісне шифрування, які й сьогодні є авангардом криптографічної науки.

Актуальною залишається і вдосконалення симетричних та асиметричних криптосистем. Було розроблено нефейстелівські симетричні криптоалгоритми (SAFER, RC4-RC6 тощо), альтернативні асиметричні системи (ЕльГамаль, Меркл-Хеллман тощо). В Україні зараз очікується бум криптографічних технологій. Окрім ГОСТ 28147-89, сертифікованого ще за часів Радянського Союзу симетричного алгоритму, починається розробка асиметричних алгоритмів для виконання електронного цифрового підпису та створення умов електронного документообігу. Наприклад, програмно-технічний комплекс центру сертифікації ключів професора Горбенко І.Д. був нагороджений почесною відзнакою Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України та рекомендований до використання державними службами України, які переходять до електронної звітності. Криптографічний алгоритм професора Горбенка І.Д. використовує кінцеву групу еліптичної кривої над кінцевим полем Галуа.