Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

ЛЕКЦІЯ №5

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ПИТАННЯ:

1. ІСТОРИЧНА ДОВІДКА.
2. ОСНОВНІ ПОНЯТТЯ КРИПТОГРАФІЇ.
3. ШИФРУВАННЯ КЛЮЧЕМ. СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ. ГІБРИДНЕ ТА КВАНТОВЕ ШИФРУВАННЯ.
4. ПОНЯТТЯ КРИПТОРГАФІЧНОЇ СИСТЕМИ.

ПИТАННЯ №1

ІСТОРИЧНА ДОВІДКА

Криптографія, наука про написання кодів і шифрів для безпечного зв'язку, є одним з найбільш важливих елементів, який уможливлює появу сучасних криптовалют і блокчейнів. Однак криптографічні методи, які використовуються сьогодні, є результатом неймовірно довгої історії розвитку. З давніх часів люди використовували криптографію для безпечної передачі інформації. Багатолітня історія криптографії призвела до появи передових і складних методів, що використовуються для сучасного цифрового шифрування.

Історія криптографії налічує близько 4 тисяч років. Як основний критерій періодизації криптографії можна взяти технологічні характеристики використовуваних методів шифрування.

До нашого часу криптографія займалася виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) – перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотне відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного знання (а саме ключа, необхідного для дешифровки повідомлення). В останні десятиліття 21 сторіччя сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування тощо.

ДАВНЄ КОРІННЯ КРИПТОГРАФІЇ

Відомо, що примітивні криптографічні методи існували в давнину, і більшість ранніх цивілізацій, схоже, тією чи іншою мірою використовували криптографію. Заміна символів, найбільш основна форма криптографії, зустрічається як у давньоєгипетських, так і в месопотамських письменах. Перший відомий приклад цього типу криптографії було знайдено в гробниці єгипетського дворянина на ім'я **Хнумхотеп II**, який жив приблизно 3900 років тому.

Метою заміни символів у написах Хнумхотепа було не приховування інформації, а посилення її лінгвістичної привабливості. Найперший відомий приклад криптографії, що використовується для захисту конфіденційної інформації, був знайдений близько 3500 років тому, коли месопотамський писар використовував криптографію, щоб приховати формулу керамічної глазурі, яка використовувалася на глиняних табличках.

ДАВНЄ КОРІННЯ КРИПТОГРАФІЇ

У пізніші періоди античності, криптографія широко використовувалася для захисту важливої військової інформації, цій меті вона служить і до сьогодні. **У грецькому місті-державі Спарта**, повідомлення були зашифровані записом на пергаменті, який обгортали навколо циліндра певного розміру, що робило повідомлення нерозбірливим, поки одержувач не обгортав його навколо аналогічного циліндра. Також відомо, що шпигуни в стародавній Індії використовували закодовані повідомлення ще у 2 столітті до нашої ери.

Найімовірніше, що найдосконаліша криптографія у стародавньому світі була досягнута римлянами. Яскравий приклад римської криптографії, відомої як **шифр Цезаря**, використовував зміщення літер зашифрованого повідомлення на ті, що йдуть на декілька місць пізніше у латинському алфавіті. Знаючи цю систему та кількість місць для перестановки букв, одержувач міг успішно розшифрувати повідомлення.

РОЗВИТОК В ЕПОХУ СЕРЕДНЬОВІЧЧЯ ТА ВІДРОДЖЕННЯ

У середньовіччі криптографія ставала дедалі більш просунутою, але шифри заміщення, прикладом яких є шифр Цезаря, залишалися стандартом. ***Криптоаналіз*** – наука, за допомогою якої зламуються коди та шифри, почала наздоганяти все ще відносно примітивну науку криптографії. **Аль-Кінді**, відомий арабський математик, розробив метод, відомий як **частотний аналіз**, приблизно у 800 р. н.е., який зробив шифри заміщення вразливими для дешифрування. Тоді люди, які намагаються розшифрувати зашифровані повідомлення, вперше отримали доступ до систематичного методу, що дозволяє криптографії просуватися ще далі та бути корисною.

У 1465 році **Леоне Альберті** розробив **поліалфавітний шифр**, який вважається рішенням проти методу частотного аналізу Аль-Кінді. У поліалфавітному шифрі повідомлення кодується за допомогою двох різних алфавітів. Перший – це алфавіт, де написано вихідне повідомлення, а другий – це зовсім інший алфавіт, у якому повідомлення з'являється після кодування. У поєднанні з традиційними шифрами заміни, поліалфавітні шифри значно підвищують безпеку закодованої інформації. Якщо читач не знав алфавіту, в якому спочатку було написано повідомлення, метод частотного аналізу був марним.

Нові методи кодування інформації були розроблені в епоху Відродження, зокрема популярний **метод двійкового кодування**, винайдений знаменитим ерудитом сером **Френсісом Беконом** у 1623 році.

XIX СТОЛІТТЯ

В **поліалфавітному шифрі Віженера** (англ. Vigenère cipher), алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині 1800-тих, **Чарльз Беббідж** показав, що **поліалфавітні шифри цього типу залишились частково беззахисними перед частотним аналізом**.

Хоча частотний аналіз є потужною та загальною технікою, шифрування, на практиці, часто було ефективним; багато із криптоаналітиків не знали цю техніку. Дешифрування повідомлень без частотного аналізу практично означало необхідність знання використаного шифру, спонукаючи, таким чином, до шпигунства, підкупу, крадіжок, зрад, тощо для отримання алгоритму. Згодом, в XIX-тому столітті, було визнано, що збереження алгоритму шифрування в таємниці не забезпечує захист від зламу; насправді, було встановлено, що будь-яка адекватна криптографічна схема залишається у безпеці, навіть за умови доступу сторонніх. Збереження в таємниці ключа має бути достатньою умовою захисту інформації нормальним шифром. Цей фундаментальний принцип було вперше проголошено в 1883 **Огюстом Керкгофсом**, і загальновідомий як ***принцип Керкгоффза***; різкіший варіант озвучив **Клод Шеннон** як ***максиму Шеннона*** – ворог знає систему.

Було створено різні **механічні прилади та інструменти** для допомоги в шифруванні. Одним з найперших є ***скітала*** в стародавній Греції, палиця, що, як вважається, використовувалась Спартанцями як перестановочний шифр. В середньовіччя, було винайдено інші засоби, такі як ***дірочний шифр***, що також використовувався для часткової стеганографії. Разом із винаходом поліалфавітних шифрів, було розроблено досконаліші засоби, такі як власний винахід Альберті ***шифрувальний диск***, ***табула ректа*** Йогана Тритеміуса, та ***мультициліндр*** Томаса Джефферсона (повторно винайдений Базерієсом приблизно в 1900 році).

ДОСЯГНЕННЯ ОСТАННІХ СТОЛІТЬ

Криптографія продовжувала активно прогресувати протягом століть. Великий прорив у криптографії був описаний **Томасом Джефферсоном** у 1790-х роках, хоча, можливо, так не був реалізований. Його винахід, відомий як ***колесо шифрування***, складався з 36 кілець з літерами на рухомих колесах, які можна використовувати для досягнення складного кодування. Ця концепція була настільки розвинена, що стала основою для американської військової криптографії аж до Другої світової війни.

Друга світова війна також побачила чудовий приклад аналогової криптографії, відомої як машина ***Енігма***. Подібно до колеса шифрування, цей пристрій, що використовувався Німеччиною, використовував колеса, які оберталися для кодування повідомлення, що робило практично неможливим читання без іншого пристрою Енігма. Ранні комп'ютерні технології зрештою використовувалися, щоб допомогти зламати шифр Енігма. Успішне дешифрування повідомлень Енігма вважається найважливішим компонентом перемоги союзників.

КРИПТОГРАФІЯ В КОМП'ЮТЕРНУ ЕРУ

З появою комп'ютерів криптографія стала більш просунутою, ніж в аналогову епоху. 128-бітове математичне шифрування, надійніше, ніж будь-який древній або середньовічний шифр, тепер є стандартом для багатьох пристроїв та комп'ютерних систем. Починаючи з 1990 року, вчені розробляли зовсім нову форму криптографії, яку називають квантовою криптографією, сподіваючись ще раз підвищити рівень захисту сучасного шифрування.

Нещодавно криптографічні методи також почали використовуватися для створення криптовалют. Криптовалюти використовують кілька передових криптографічних методів, зокрема хеш-функції, криптографію з публічним ключем та цифрові підписи. Ці методи використовуються головним чином для забезпечення безпеки даних, що зберігаються в блокчейні, а також для автентифікації транзакцій. Спеціалізована форма криптографії, відома як алгоритм цифрового підпису еліптичної кривої (ECDSA), лежить в основі Bitcoin та інших криптовалютних систем як засіб забезпечення додаткової безпеки та гарантії того, що коштами можуть користуватися лише їхні законні власники.

Криптографія пройшла довгий шлях за останні 4000 років, і навряд чи вона зупиниться. Поки конфіденційні дані вимагають захисту, криптографія продовжуватиме розвиватися. Криптографічні системи, що використовуються у криптовалютних блокчейнах сьогодні, є однією з найбільш просунутих форм цієї науки. Вони також є частиною традиційної історії людства.

ПИТАННЯ №2

ОСНОВНІ ПОНЯТТЯ КРИПТОГРАФІЇ

ОСНОВНІ ПОНЯТТЯ

Криптографія (англ. – cryptography) – це наука, що займається вивченням та розробленням методів, способів та засобів перетворення інформації у вигляд, який ускладнює чи унеможливлює несанкціоновані дії з нею. Криптографія базується на методах (алгоритмах) шифрування та дешифрування.

Шифрування (англ. – encryption) – це процес криптографічного перетворення даних, за допомогою якого відкритий текст перетворюється на шифрований з метою захисту від несанкціонованого доступу.

Дешифрування (англ. – decryption) – це процес, зворотний шифруванню.

Алгоритм шифрування (англ. – encryption algorithm) – це алгоритм, згідно з яким здійснюється спеціальне криптографічне перетворення інформації (його ще називають криптографічним алгоритмом або криптоалгоритмом).

ОСНОВНІ ПОНЯТТЯ

Криптоаналіз (англ. – cryptanalysis) – наука, що займається вивченням та розробленням методів, способів та засобів розкриття шифрів.

Стеганографія (англ. – stegonography) – набір засобів і методів приховування факту передавання повідомлення.

Криптологія (англ. – cryptology) – наука, складовими якої є криптографія, криптоаналіз та, за деякими визначеннями, стеганографія.

Незаперечність причетності до авторства – це поняття, зворотне поняттю відмови від авторства, тобто заперечення причетності до створення або передавання якого-небудь документа чи повідомлення. У свою чергу, *незаперечність причетності до одержання документа або повідомлення* – поняття, зворотне поняттю відмови від причетності до одержання будь-якого документа чи повідомлення.

ОСНОВНІ ПОНЯТТЯ

Важливим поняттям криптографії є ***криптоаналітична атака*** (англ. – cryptoanalytic attack) – це загальна назва методу, за допомогою якого криптоаналітик намагається зламати криптосистему.

У криптографії використовують поняття ***стійкість криптографічних алгоритмів*** (англ. – cipher strength), яке характеризує рівень стійкості криптоалгоритму до його зламу. Стійкість визначається кількістю часу та обчислювальними ресурсами, необхідними для розшифрування криптоалгоритму. Розрізняють *абсолютну* й *практичну стійкість криптоалгоритмів*.

Абсолютна стійкість криптоалгоритмів (англ. – perfect secrecy) – означає (за Шенноном) статистичну незалежність відкритого та зашифрованого текстів, якої можна досягти, наприклад, за умови, що ключ має довжину, не меншу за довжину відкритого тексту, та що його обрано з простору ключів справді випадково і буде використано лише один раз.

Практична стійкість криптоалгоритмів (англ. – computationally secure) – це поняття стійкості алгоритмів, які не є ідеальними, тобто можуть бути дешифрованими за скінченний час.

ОСНОВНІ ПОНЯТТЯ

У сучасній криптографії криптографічні методи не використовують кожний окремо, вони є основою для більш загальної криптографічної системи.

Криптографічна система, або ***криптосистема*** (англ. – cryptosystem) – це сукупність програмних, апаратних, програмно-апаратних засобів, а також криптографічних алгоритмів або криптографічних схем і ключових параметрів, об'єднаних в єдину систему з метою розв'язання конкретної задачі захисту інформації.

Тайнопис (англ. – cryptographic writing) – це методи кодування, особливістю яких є обов'язкове збереження в таємниці криптографічного алгоритму від третьої сторони, що певним чином обмежує їх функціональні можливості. У сучасній криптографії такі методи не використовують.

Шифрування з ключем (англ. – key coding) – це методи кодування, коли ключ зберігається в таємниці від третьої сторони (зберігати криптографічний алгоритм у цьому випадку не потрібно).

Стандарт шифрування (англ. – encryption standard) – це повний опис алгоритму шифрування (та правил його використання), призначеного для програмної або апаратної реалізації, обов'язкового для використання організаціями, які зазначені в цьому стандарті.

ПИТАННЯ №3

ШИФРУВАННЯ КЛЮЧЕМ. СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ. ГІБРИДНЕ ТА КВАНТОВЕ ШИФРУВАННЯ

ВИДИ АЛГОРИТМІВ ШИФРУВАННЯ

Алгоритми шифрування з ключем поділяють на дві великі групи: *алгоритми симетричного шифрування* і *алгоритми асиметричного шифрування*.

Симетричне шифрування (англ. – symmetric coding) – це метод, за якого ключі шифрування і розшифрування або однакові, або легко виводяться один з одного, забезпечуючи таким чином спільний ключ, який є таємним.

Асиметричне шифрування (англ. – asymmetric coding) – набір методів криптографічного шифрування, в яких використовують два ключі – таємний (приватний) і відкритий; жоден із ключів не може бути обчислений з іншого за прийнятний час. Таке шифрування ще називають *шифруванням з відкритим ключем* (англ. - public key coding).

СИМЕТРИЧНЕ ШИФРУВАННЯ

Основне призначення симетричних криптоалгоритмів – шифрування великих масивів даних із великою швидкістю.

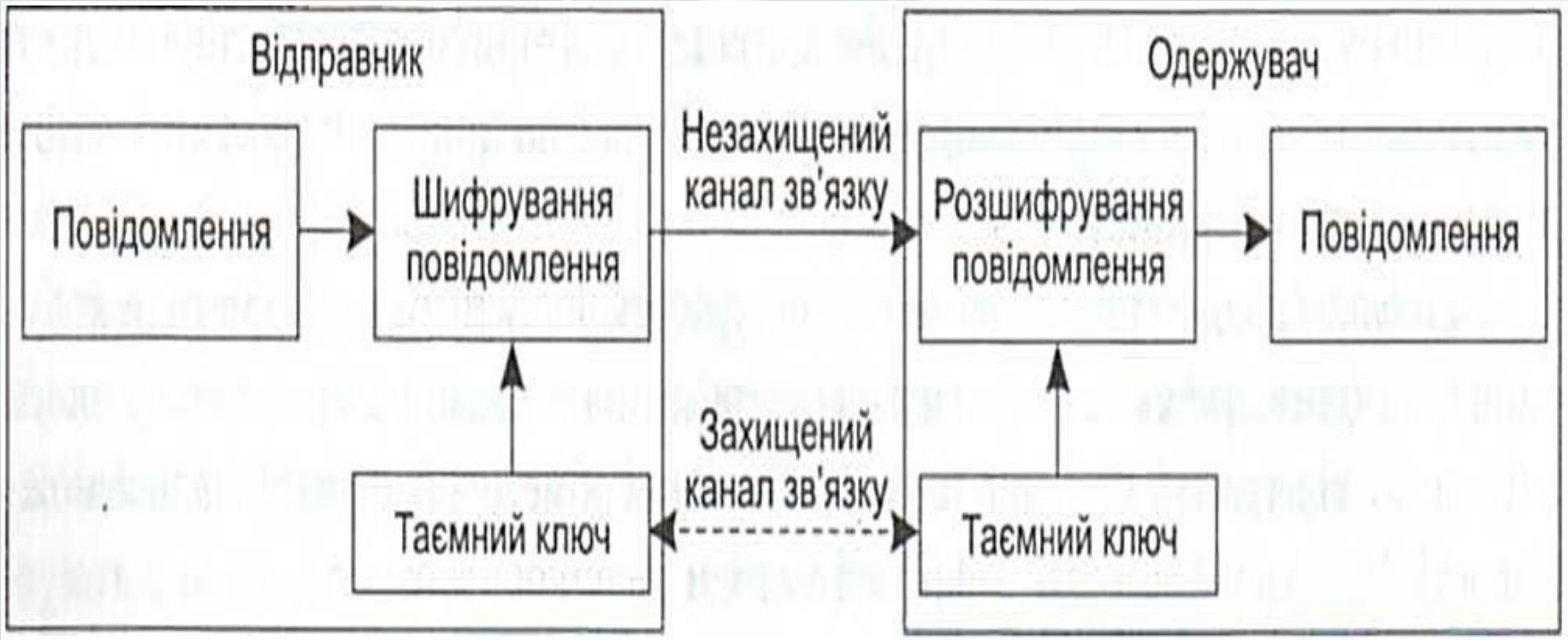

Рис.1.Структурна схема шифрування на таємному ключі

ВИДИ СИМЕТРИЧНИХ АЛГОРИТМІВ

Потокове шифрування (англ. – stream coding) – це спосіб шифрування даних, коли кожний знак шифрується окремо. Цей криптоалгоритм обробляє інформацію посимвольно, тому, користуючись ним, можна послідовно шифрувати та розшифровувати інформацію будь-якого обсягу. Таке шифрування застосовують переважно в каналах зв'язку.

Блокове шифрування (англ. – block coding) – спосіб шифрування даних, коли кожний блок, що передається, може шифруватися окремо. Блоковий шифр - процедура відображення множини вхідних блоків вихідного тексту на множину блоків зашифрованого тексту. Блоки вихідних даних можуть налічувати від одного до кількох сотень бітів. У сучасних системах блокового шифрування використовують блоки з 64, 128, 192 або 256 біт. Алгоритми блокового шифрування – це комбінація оборотних криптоперетворень, які виконуються багаторазово.

До деяких відомих, поширених алгоритмів з гарною репутацією належать: Twofish, Serpent, AES (або Рейндайль), Blowfish, CAST5, RC4, TDES (3DES), та IDEA.

АСИМЕТРИЧНЕ ШИФРУВАННЯ

Головне досягнення асиметричного шифрування в тому , що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпала. Процедура шифрування обрана так, що вона необоротна навіть по відомому ключу шифрування. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення – прочитати його можна тільки за допомогою другого ключа – ключа дешифрування. А раз так, то ключ шифрування для відправлення листів якій-небудь особі можна взагалі не приховувати – знаючи його однаково неможливо прочитати зашифроване повідомлення. Тому, ключ шифрування називають в асиметричних системах ***“відкритим ключем”***, а от ключ дешифрування одержувачеві повідомлень необхідно тримати в секреті – він називається ***“закритим ключем”***. Алгоритми шифрування й дешифрування створюються так, щоб знаючи відкритий ключ, неможливо було обчислити закритий ключ.

АСИМЕТРИЧНЕ ШИФРУВАННЯ

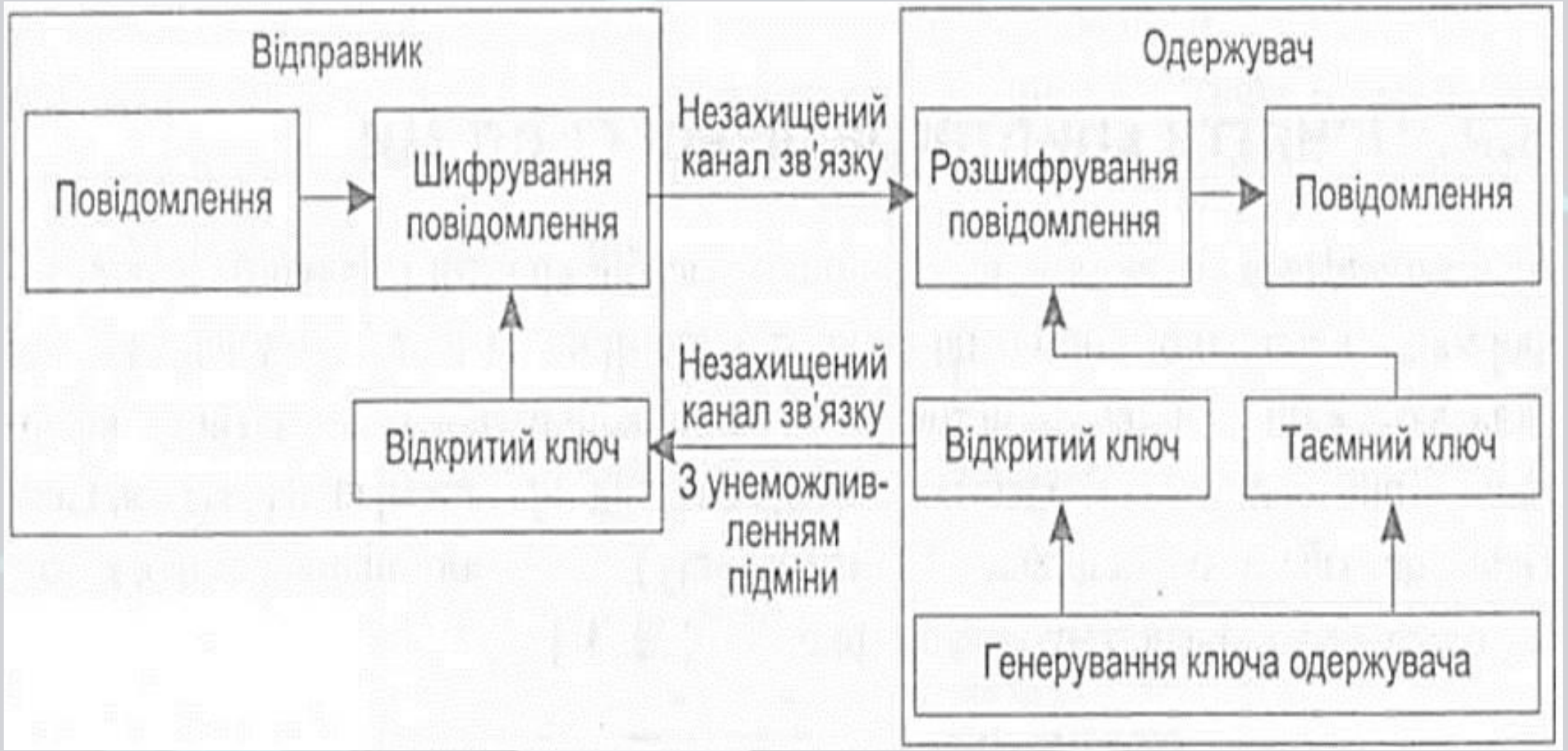

Рис.2.Структурна схема шифрування на відкритому ключі

АСИМЕТРИЧНЕ ШИФРУВАННЯ

Початок асиметричним шифрам було покладено в роботі «Нові напрямки в сучасній криптографії» **Вітфілда Діффі та Мартіна Геллмана**, опублікованій в 1976 році. Перебуваючи під впливом роботи **Ральфа Меркле** про поширення відкритого ключа, вони запропонували метод отримання секретних ключів, використовуючи відкритий канал. Цей метод експоненціального обміну ключів, який став відомий як обмін ключами Діффі-Геллмана, був першим опублікованим практичним методом для встановлення поділу секретного ключа між завіреними користувачами каналу. У 2002 році Геллман запропонував називати даний ***алгоритм «Діффі – Геллмана – Меркле»***, визнаючи внесок Меркле в винахід криптографії з відкритим ключем. Ця ж схема була розроблена Малькольмом Вільямсоном в 1970-х, але трималася в секреті до 1997 року. Метод Меркле з розповсюдження відкритого ключа був винайдений в 1974 році і опублікований в 1978, його також називають загадкою Меркле.

У 1977 році вченими **Рональдом Рівестом, Аді Шамір і Леонардом Адлеманом** з Массачусетського Технологічного Інституту (MIT) був розроблений алгоритм шифрування, заснований на проблемі про розкладання на множники. Система була названа за першими літерами їхніх прізвищ. Ця ж система була винайдена Кліффордом Коксом в 1973 році, що працював в центрі урядового зв'язку (GCHQ). Але ця робота зберігалася лише у внутрішніх документах центру, тому про її існування було не відомо до 1977 року. ***RSA*** став першим алгоритмом, придатним і для шифрування, і для цифрового підпису.

АСИМЕТРИЧНЕ ШИФРУВАННЯ

Сучасна асиметрична криптографія базується на алгоритмах **Ель-Гамаля** (запропонованому в 1985 році) та **Міллера–Коблиця** (запропонованому в 1986 році).

Теоретичну основу стійкості алгоритму RSA становить *проблема факторизації великих цілих чисел*, а алгоритмів ЕльГамаля та Міллера–Коблиця – *проблема дискретного логарифмування*. Сьогодні відомі численні вразливості цих алгоритмів. На зміну алгоритмам шифрування на відкритому ключі прийшли більш стійкі алгоритми шифрування на еліптичних кривих, запропоновані окремо В. Міллером і Н. Коблицем у 1986 році.

Отже, **прикладами криптосистем з відкритим ключем є** Схема Ель-Гамаля (названа на честь автора, Тахера Ель-Гамаля), RSA (названа на честь винахідників: Рона Рівеста, Аді Шаміра і Леонарда Адлмана), Діффі-Геллмана і DSA, англ. Digital Signature Algorithm (винайдений Девідом Кравіцом).

ГІБРИДНЕ ТА КВАНТОВЕ ШИФРУВАННЯ

Гібридне шифрування поєднує симетричне і асиметричне шифрування для отримання кращої ефективності і безпеки. У цьому підході симетричне шифрування використовується для шифрування великих обсягів даних, а асиметричне шифрування – для захисту ключів симетричного шифрування. Ключ симетричного шифрування генерується тимчасово і шифрується за допомогою публічного ключа отримувача, після чого передається разом із зашифрованими даними.

Квантове шифрування базується на принципах квантової фізики і використовує квантові біти (кубіти) для передачі та захисту інформації. Воно забезпечує вищий рівень безпеки, оскільки будь-яке спроби перехопити чи скомпрометувати передачу даних виявляється. **Основи квантової криптографії включають** квантову телепортацію, квантовий обмін ключами і квантову стійкість. Деякі приклади квантових шифрів включають BB84, E91 і B92.

СФЕРИ ЗАСТОСУВАННЯ АЛГОРИТМІВ АСИМЕТРИЧНОГО ШИФРУВАННЯ

Алгоритми асиметричного шифрування, так само як і симетричного, застосовують для шифрування масивів даних, але їхня швидкість значно нижча. Основне призначення асиметричних алгоритмів – забезпечення ефективного функціонування сучасних криптосистем. Саме ці алгоритми покладено в основу задач автентифікації користувачів, контролю цілісності інформації, унеможливлення відмови від авторства чи факту одержання даних тощо.

Електронно-цифровий підпис (англ. – electronic digital signature) – цифрова послідовність, що додається до повідомлення (даних) для забезпечення цілісності інформації та підтвердження авторства і формується із застосуванням асиметричних криптосистем.

ПИТАННЯ №4

ПОНЯТТЯ КРИПТОРГАФІЧНОЇ СИСТЕМИ

КРИПТОГРАФІЧНА СИСТЕМА

Криптографічна система – це сукупність засобів криптографічного захисту інформації, необхідної нормативної, експлуатаційної та іншої документації, які складають єдину систему з метою розв'язання конкретної задачі захисту інформації.

Криптосистема складається з таких базових підсистем: шифрування, ідентифікації, забезпечення цілісності (імітозахисту), цифрового підпису тощо, кожна з яких має свою підсистему ключів(рис.3).

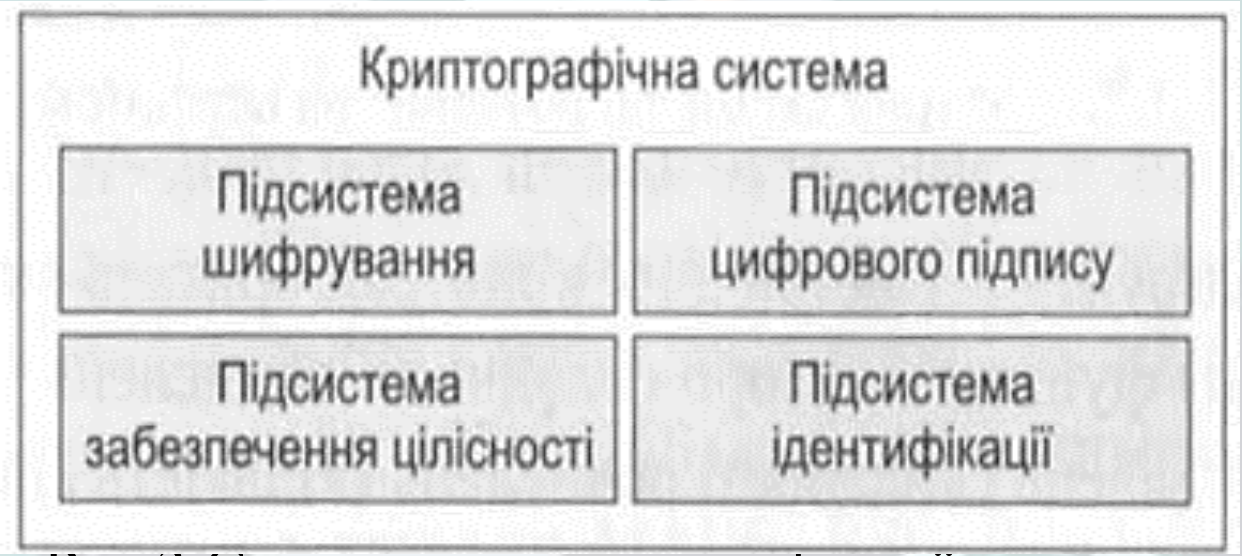

Рис.3.Структура криптографічної системи

ПІДСИСТЕМА ШИФРУВАННЯ

Підсистема шифрування виконує функції шифруваннярозшифрування даних, її основу складають шифр та підсистема ключів (рис. 4).

Шифр, що базується на відповідному криптоалгоритмі, містить модель відкритого тексту. Як уже зазначалося, підсистема шифрування має також підсистему ключів, що буде визначена нижче.

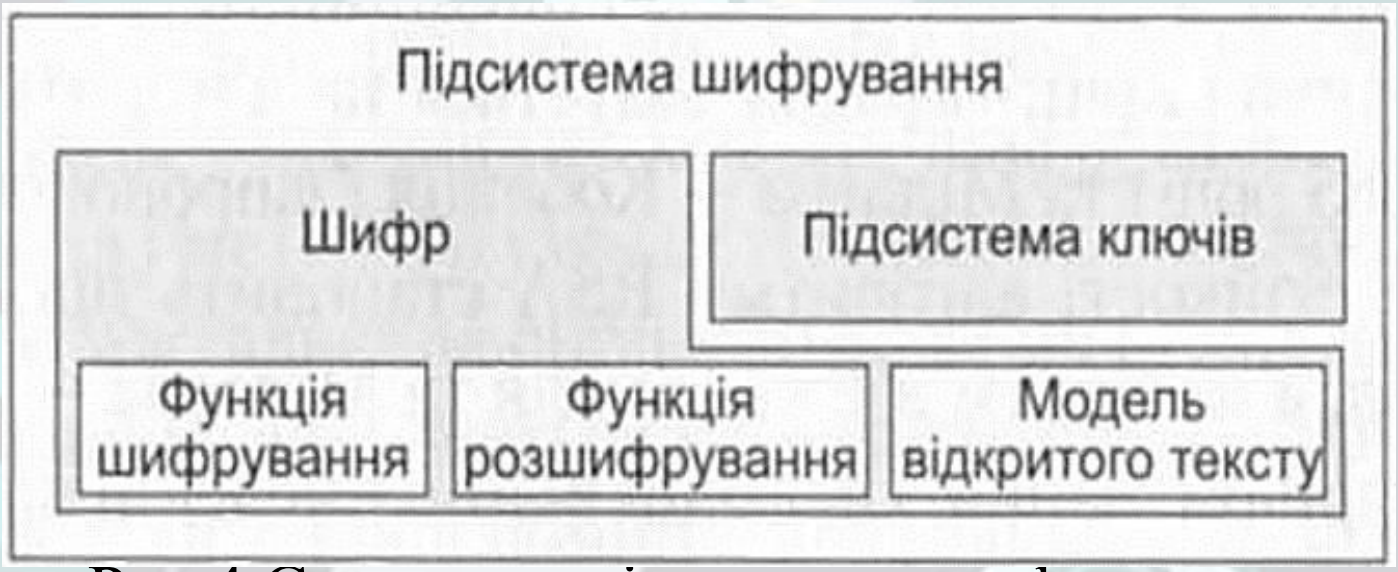

Рис.4.Структура підсистеми шифрування

ПІДСИСТЕМА ЦИФРОВОГО ПІДПИСУ

Підсистема цифрового підпису (рис. 5) виконує функцію автентифікації джерела повідомлення або документа та унеможливлює відмову суб'єктів від здійснених ними дій. Підсистема базується на схемі цифрового підпису та підсистемі ключів. Основними елементами схеми цифрового підпису є алгоритми формування та перевірки цифрового підпису.

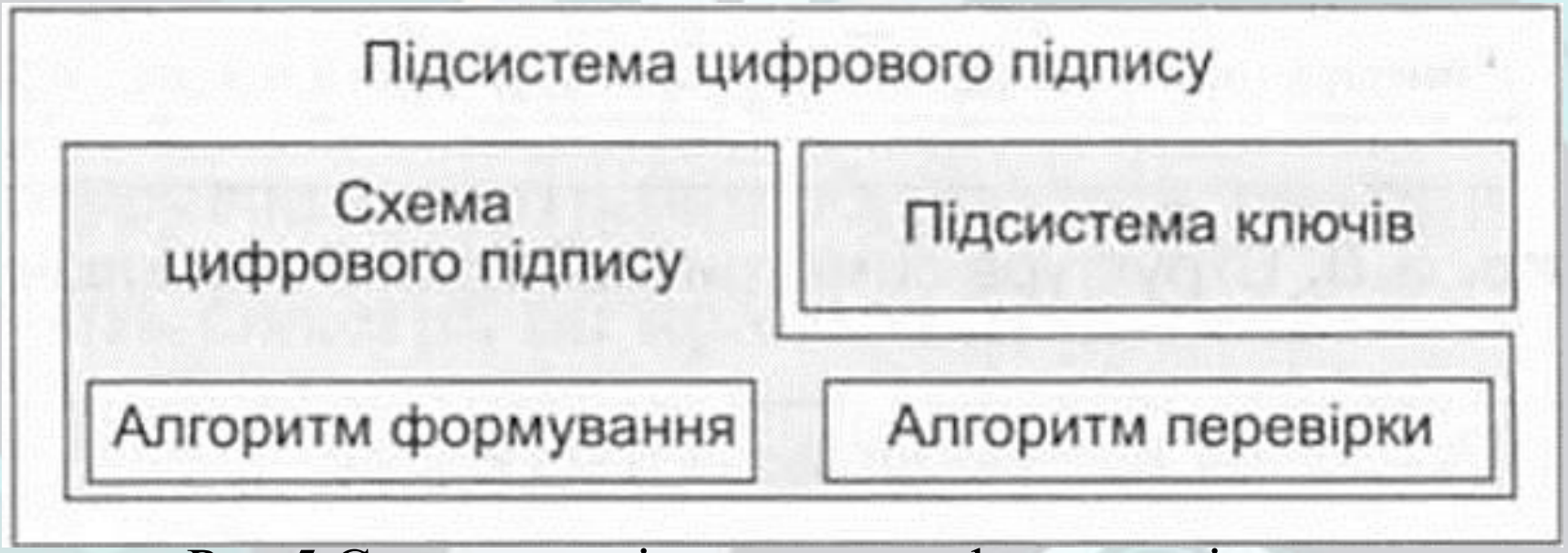

Рис.5.Структура підсистеми цифрового підпису

ПІДСИСТЕМА ІДЕНТИФІКАЦІЇ

Підсистема ідентифікації (рис. 6) забезпечує виконання операції захищеного розпізнавання суб'єктів та об'єктів доступу за їхніми ідентифікаторами. Основу цієї підсистеми складають односторонній або взаємний протокол ідентифікації, а також підсистема ключів.

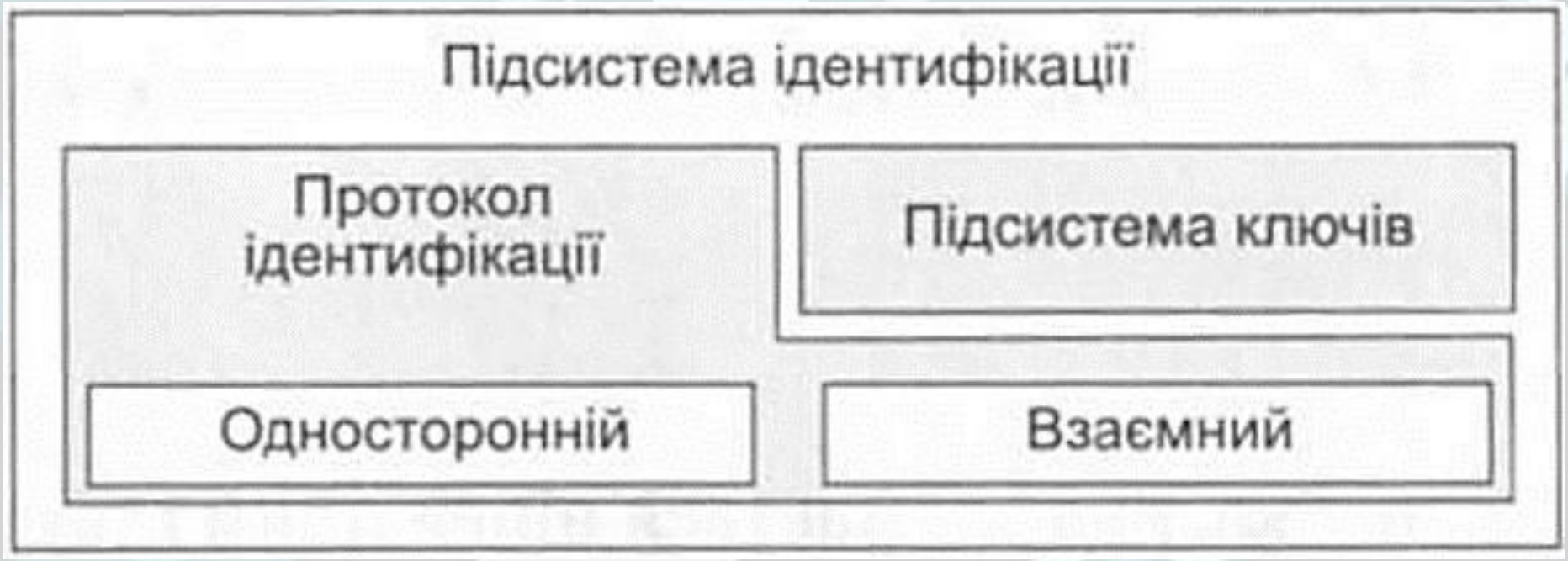

Рис.6.Структура підсистеми ідентифікації

ПІДСИСТЕМА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

Підсистема забезпечення цілісності інформації (імітозахист) (рис.7) захищає її від несанкціонованого модифікування і перешкоджає нав'язуванню фальшивих відомостей. Підсистема базується на відповідному алгоритмі забезпечення цілісності інформації та підсистемі ключів. У свою чергу, забезпечення цілісності інформації здійснюється шляхом використання алгоритму шифрування, автентифікаційного коду та інших засобів.

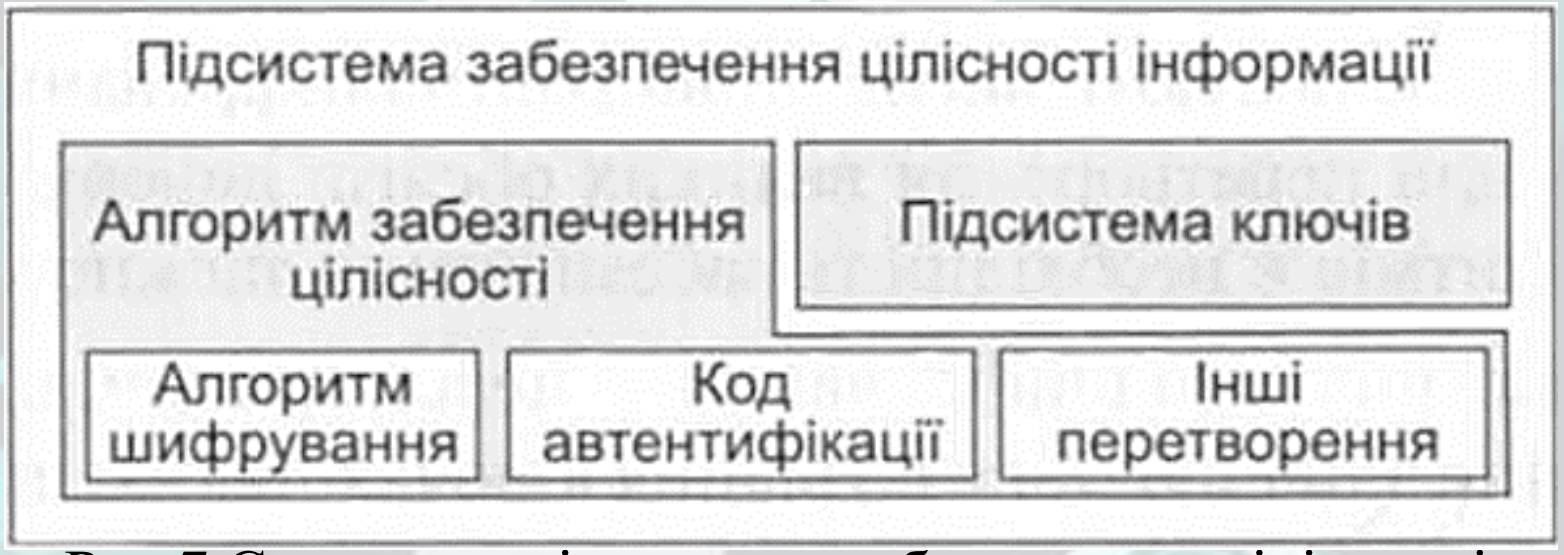

Рис.7.Структура підсистеми забезпечення цілісності

ПІДСИСТЕМА КЛЮЧІВ

Підсистема ключів визначає порядок функціонування підсистем, до складу яких вона входить. **Розрізняють симетричні та асиметричні підсистеми ключів:** підсистеми, де використовують алгоритми симетричного шифрування (шифрування з таємним ключем), та підсистеми, в яких застосовують алгоритми асиметричного шифрування (шифрування з відкритим ключем).

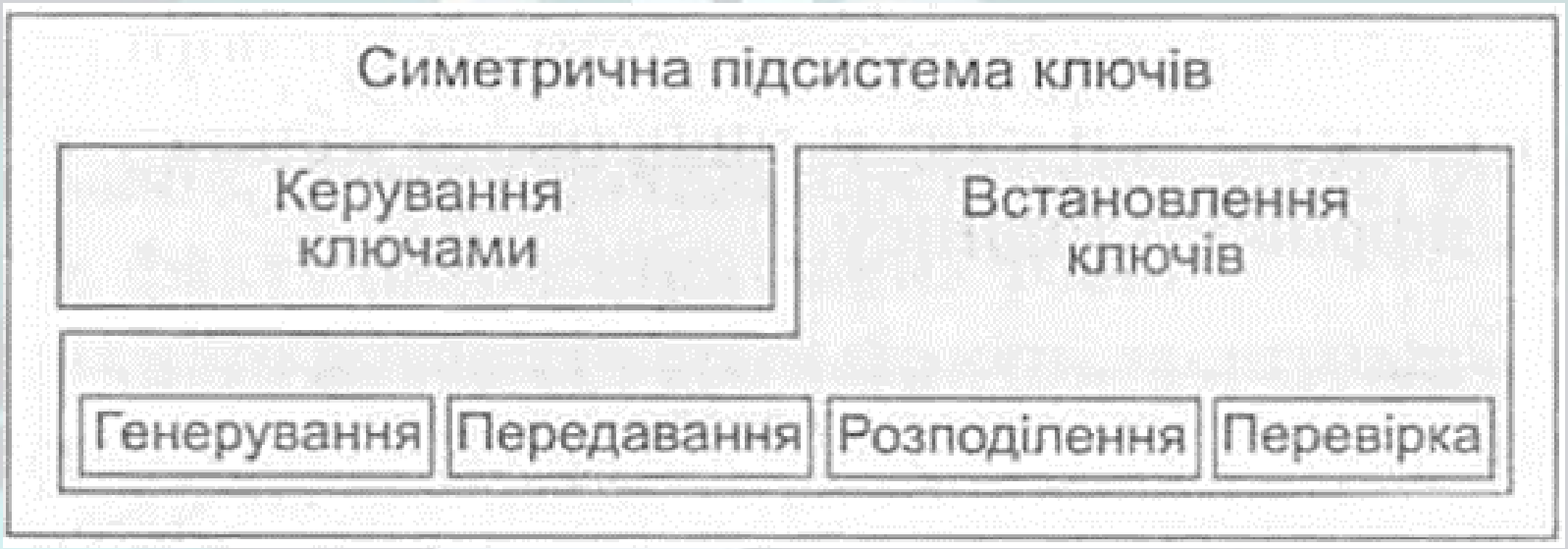

Рис.8.Структура симетричної підсистеми ключів

ПІДСИСТЕМА КЛЮЧІВ

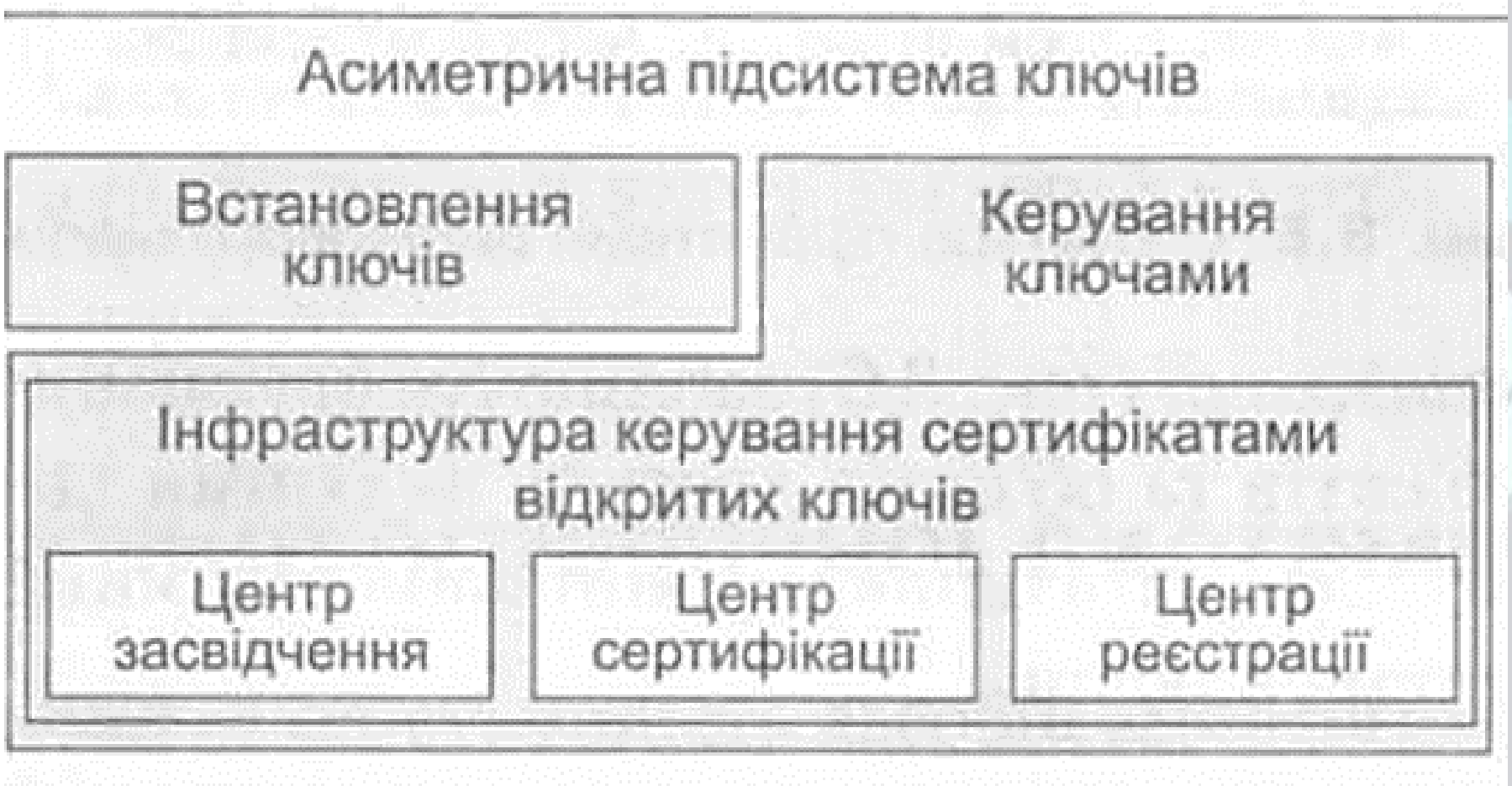

Рис.9.Структура асиметричної підсистеми ключів

ДЯКУЮ ЗА УВАГУ!