Теоретичні основи захисту інформації

Самостійна робота №2

Перевірив:

_____

Виконав:

студент II курсу

групи ФБ-01

Сахній Н.Р.

Завдання 1.

Для системи з рольовим керуванням доступом із заданим призначенням ролей і повноважень та ієрархією ролей знайти повноваження користувачів у вигляді матриці доступу.

$F_{UR}=\{(u_1,r_2),(u_2,r_3),(u_3,r_4),(u_4,r_5)\}$ та $F_{PR}=\{(r_1,p_1),(r_2,p_2),(r_3,p_3),(r_4,p_4),(r_5,p_5)\}$

// Додатково, щоб було зручно побачити відповідність між користувачамми та їх ролями, та між роллю та її повноваженнями можна розписати наступні таблиці:

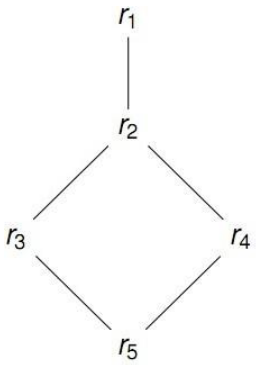
User Assignment

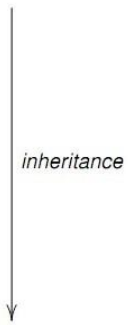
User	Role
u_1	r_2
u_2	r_3
u_3	r_4
u_4	r_5

Permission Assignment

Role	Permission
r_1	p_1
r_2	p_2 p_1
r_3	p_3 (p_2 p_1)
r_4	p_4 (p_2 p_1)
r_5	p_5 (p_4 p_3 p_2 p_1)

* У червоних дужках записанні повноваження, які були успадкувані від батьківських ролей

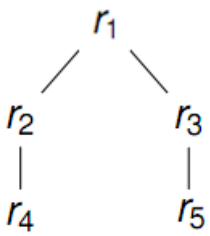




	p_1	p_2	p_3	p_4	p_5
u_1	✖	✖			
u_2	✖	✖	✖		
u_3	✖	✖		✖	
u_4	✖	✖	✖	✖	✖

Завдання 2.

Дана матриця доступу для деякої системи з рольовим керуванням доступом із заданою ієрархією ролей. Відомо, що користувач C має роль r_4. Також, будь який користувач може мати більше, аніж одну роль. Враховуючи принцип найменших повноважень, знайти розподіл ролей та повноважень для даної системи.



User Assignment

User	Role
A	r_3 r_4
B	r_2
C	r_4
D	r_5
E	r_3
F	r_2 r_5

×

Permission Assignment

Role	Permission
r_1	—
r_2	p_2 p_3
r_3	p_1 p_4
r_4	p_6 (p_2 p_3)
r_5	p_5 (p_1 p_4)

=

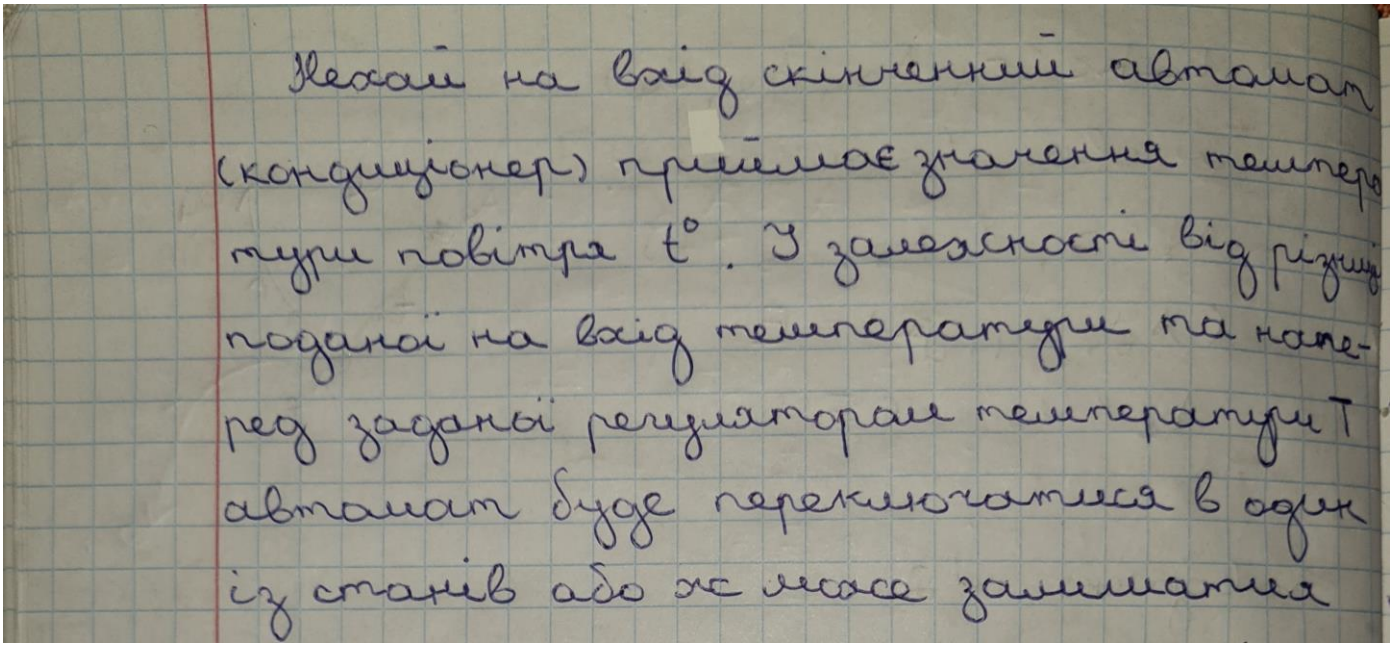
Access Matrix

	p_1	p_2	p_3	p_4	p_5	p_6
A	×	×	×	×		×
B		×	×			
C		×	×			×
D	×			×	×	
E	×			×		
F	×	×	×	×	×	

* У червоних дужках записанні повноваження, які були успадкувані від батьківських ролей

Завдання 3.

Кондиціонер вимірює поточну температуру повітря *t* один раз на хвилину та, в залежності від заданої регулятором температури T, включає один з трьох режимів охолодження: якщо різниця температур більше 7^0 — режим R_3, якщо різниця менше 7^0, але більше 3^0 — режим R_2, якщо різниця менше 3^0 — режим R_1. Виключити охолодження — режим R_0. Запишіть модель детермінованого скінченного автомату, що описує роботу кондиціонеру, у вигляді діаграми станів та матриці переходів.


Нехай на вхід скінченний автомат (кондиціонер) приймає значення температури повітря t°. У залежності від різниці поданої на вхід температури та наперед заданої регулятором температури T автомат буде переключатися в один із станів або не буде змінювати

в поточному стані. І на виході автомат видає значення 0 (нуль), якщо перемикання між станами не відбулося, та значення 1 (один), якщо відбулось перемикання (Три умови, що перемикання між станами було можливим)

$M = (S, X, Y, f, g, S_0)$ - скінченний автомат

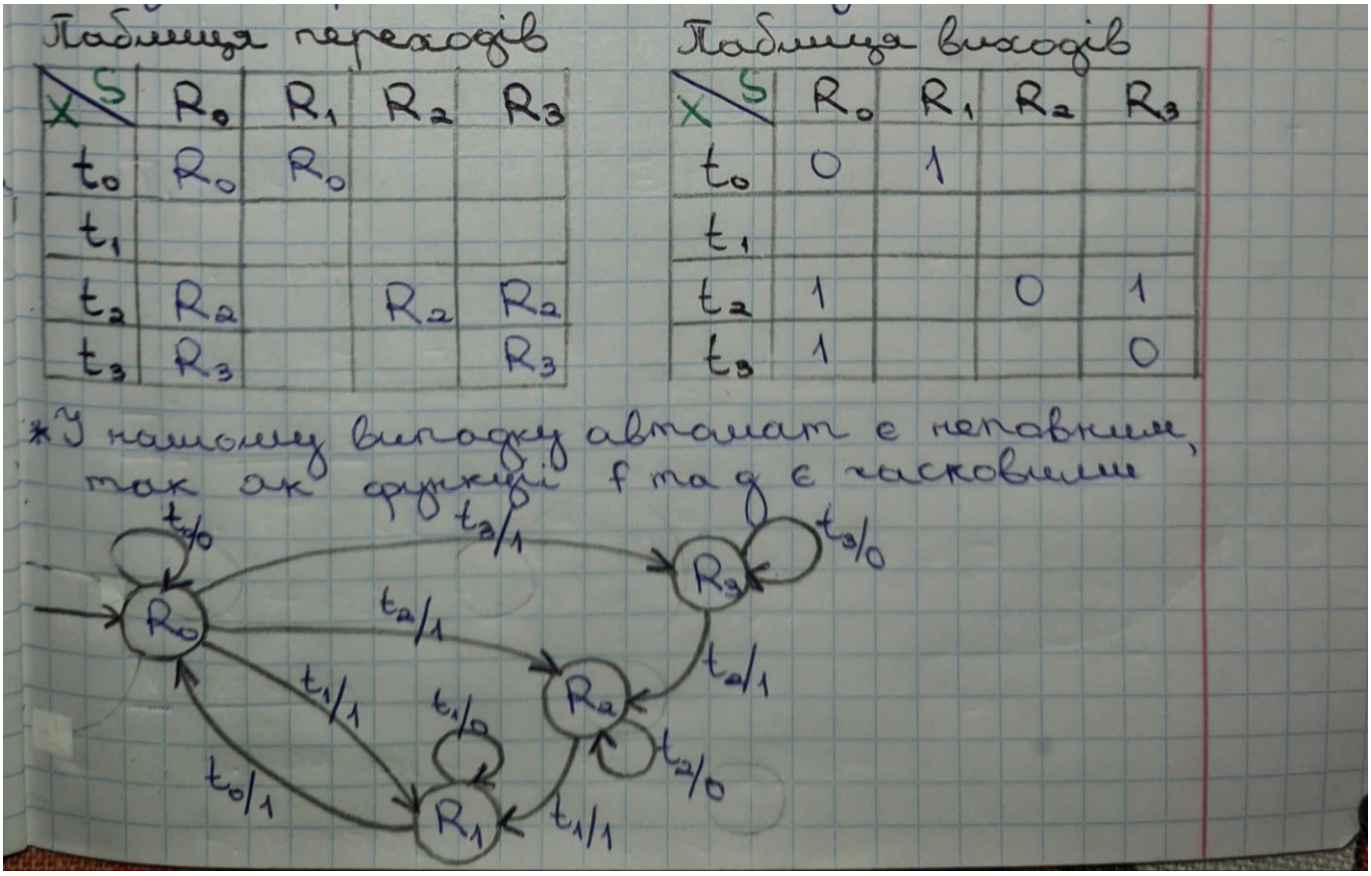
- $S = \{R_0, R_1, R_2, R_3\}$ - множина станів
- $X = \{t_0, t_1, t_2, t_3\}$ - вхідний алфавіт, де $t_0 \leq T$; $T < t_1 \leq T+3°$; $T+3° < t_2 < T+7°$; $t_3 \geq T+7°$

Тобто це множина проміжків температур повітря в залежності від заданої T —

- $Y = \{0, 1\}$ - вихідний алфавіт

- $f: S \times X \to S$ - функція переходів
- $g: S \times X \to Y$ - функція виходів
- $S_0 = R_0$ - початковий стан.

Тобто із самого початку роботи кондиціонера охолодження вимкнено, і відбувається вимір поточної температури. У залежності від температури повітря кондиціонер перейде в один із станів і почне охолоджувати повітря або ж поки не вимкнеться, коли досягне заданої регулятором температури T



Завдання 4.

Розробити та описати протокол автентифікації для автомобільної сигналізації («брелок» – «база»). Наведіть його формальний опис і модель у вигляді скінченного автомату.
(У протоколі невикористовується джерело точного часу).

- Опис протоколу автентифікації для автомобільної сигналізації:

1. **Взаємність ідентифікації.**

Одна або обидві сторони можуть підтверджувати свою особистість іншій, забезпечуючи відповідно односторонню або взаємну ідентифікацію.

2. **Ефективність обчислень.**

Уникати дорогих обчислень, коли це можливо. Щоб уникнути дорогих обчислень, краще використовувати симетричні схеми шифрування, що є для екземплярів, реалізованих шляхом використання симетричного шифрування в запущеній системі у всіх різних сценаріях.

3. **Ефективність зв'язку.**

Використовувати якомога менше протокольних повідомлень. Може бути досягнуто шляхом чергування повідомлень та уникнення зайвих кроків протоколу.

4. **Шифрування протокольних повідомлень.**

Запобігати підслуховуванню, всі протокольні повідомлення повинні бути захищені шляхом їх шифрування.

5. **Не розкривати секретних даних.**
Додатково всі секрети повинні надійно зберігатися.

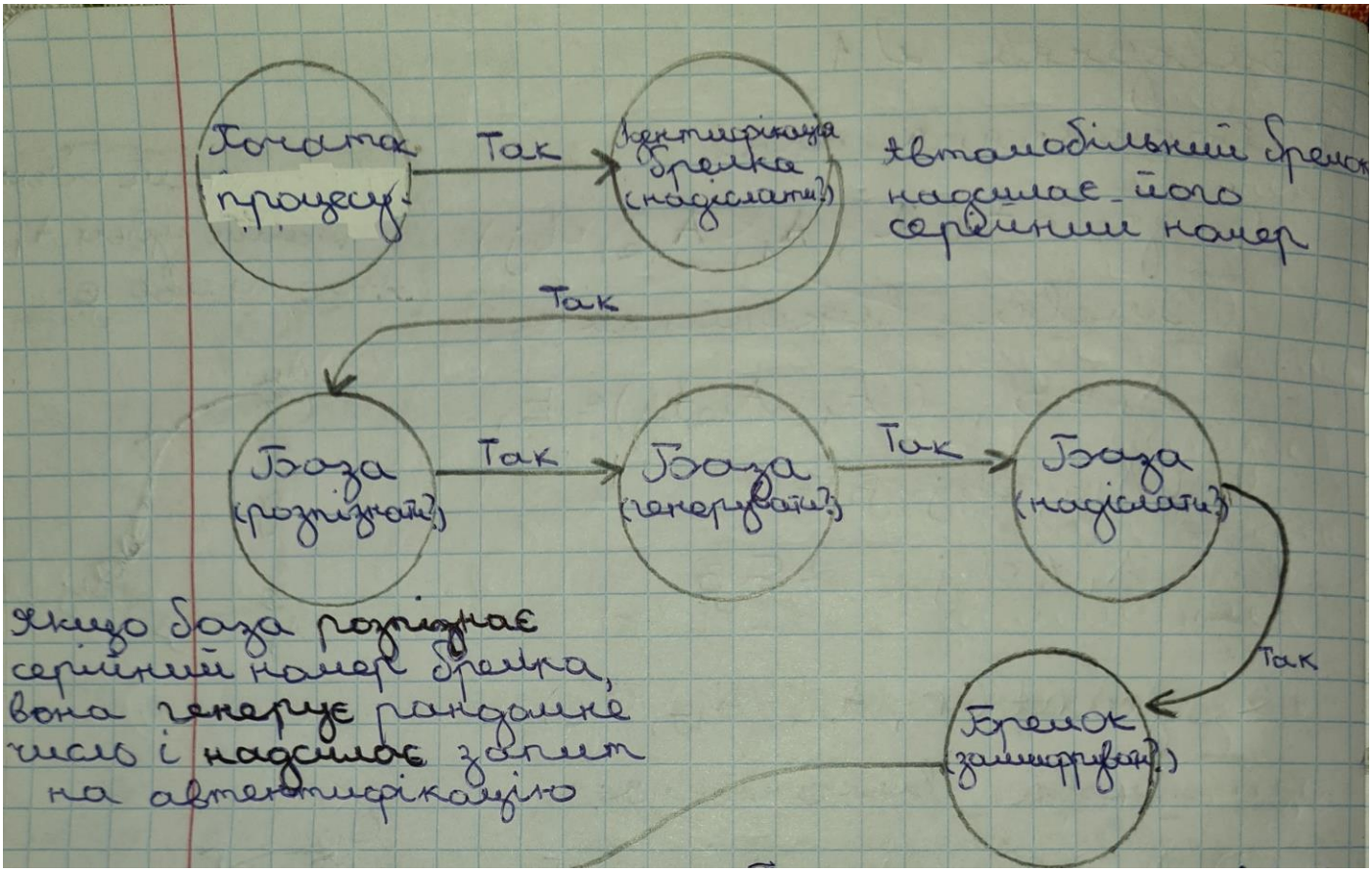
6. **Сервер знає якомога менше інформації про систему.**
Чим менше секретної інформації містить сервер, тим менше потрібно бути захищеним і тим більш незалежною є система.

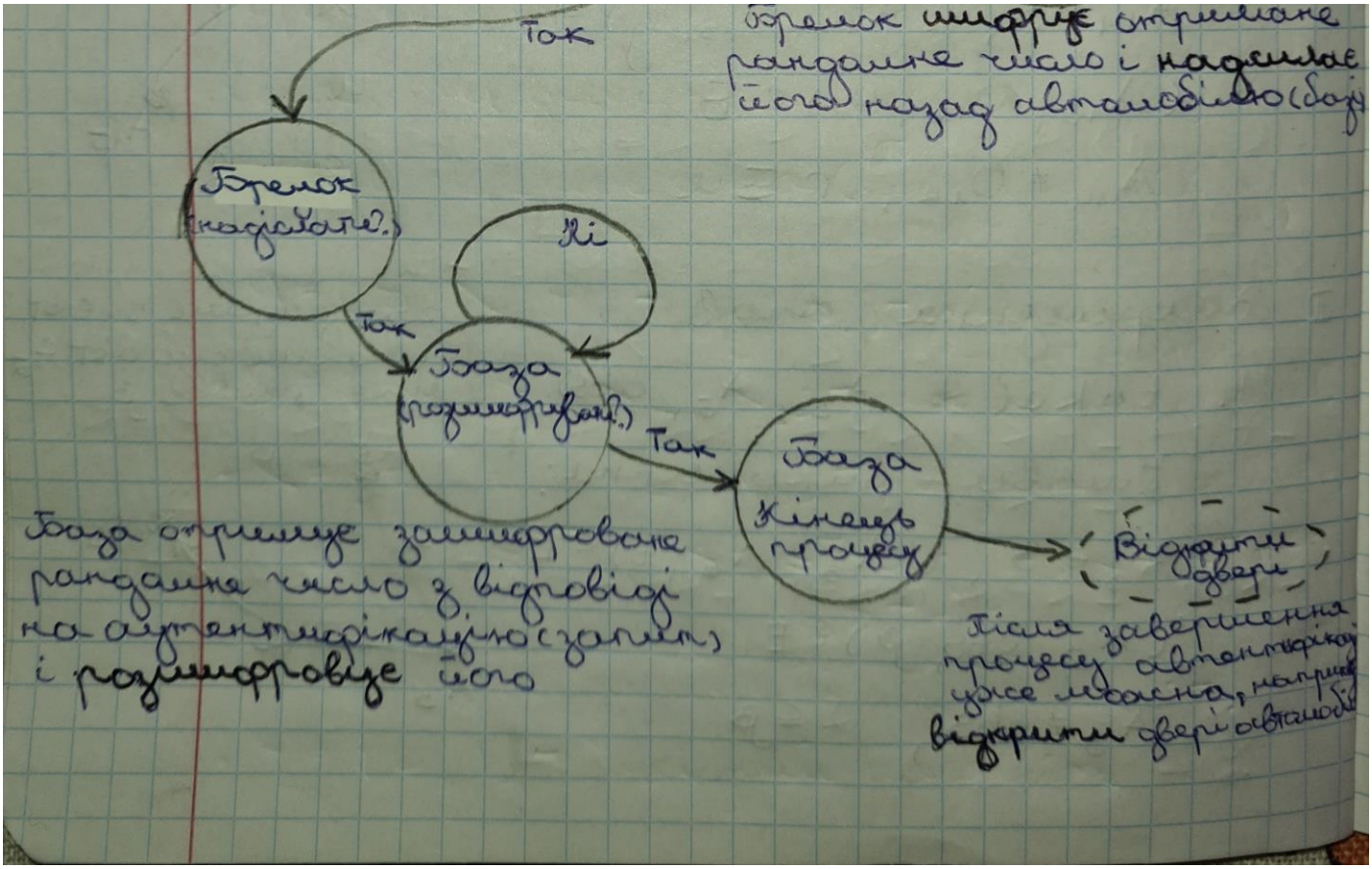
7. **Уникати використання повідомлень однакового змісту.**
Повідомлення одного і того ж протоколу ніколи не повинні містити однакові вміст і бути зашифрованим тим самим ключем, щоб уникнути атак за допомогою криптоаналізу.

8. **Підтримка неперериванння потоку протоколу.**
Можливий сценарій може полягати в тому, що компонент встановлює тривогу після очікування певного повідомлення протягом певного періоду часу.

9. **Усі асоціації тимчасові.**
Необхідно забезпечити можливість повторного використання всіх компонентів в інших системах.

- Формальний опис і модель у вигляді скінченного автомату:





Завдання 5.

Знайдіть в Інтернеті приклади атак на автомобільну сигналізацію та складіть відповідну модель загроз. На основі формальних моделей, обґрунтуйте захищеність вашого протоколу.

- Модель загроз на автомобільну сигналізацію може включати в себе такі атаки як:

1) **Пошук помилок у коді та «бекдорів»**

На сьогоднішній день це найбільша загроза для проектів, що побудовані на основі клієнт-серверної архітектури, оскільки написати повність безпечний код важко навіть для досвідчених розробників, то час від часу знаходяться нові помилки у коді, що можуть завдати суттєвої шкоди усій системі.

2) **Зламування криптоалгоритмів**

Наприклад, алгоритми для обчислення геш-функцій стандартів SHA-256 і ECDSA вважаються досить стійкими при існуючих обчислювальних потужностях. Однак, поява високопродуктивних квантових комп'ютерів збільшить ризик злому цих криптографічних функцій.

3) **Підміна даних, атака типу «маскарад»;**

Загроза підміни даних з використанням атака типу «маскарад» для отримання доступу до мережі системи безпеки автомобіля або до даних. При відсутності захисту

від такого виду атак зловмисник може провести маскування себе як авторизованого користувача (атака типу «маскарад») і здійснити несанкціонований доступ (НСД) до компонентів системи безпеки.

4) **Втрата цілісності і порушення даних сигналізації.**

Перехоплення важливих даних про роботу системи (дані про з'єднання, дані про власника, або навіть криптографічні параметри).

Система безпеки автомобіля повинна гарантувати, що всі дані, що обробляються в системі безпеки автомобіля, зберігаються та передаються, не були змінені будь-яким чином.

5) **Соціальна інженерія.**

Цей спосіб є досить вдалим для зловмисників, оскільки багато людей не розуміють її принципи роботи систем безпеки автомобіля, що дає можливість маніпулювання довірою користувачів.

У випадку з автомобільними системами безпеки може бути використано довіру власника для отримання доступу до смартфону, автомобільних ключів чи просто міток доступу автомобіля.

- Обґрунтування захищеності протоколу на основні формальних моделей

Проаналізувавши протокол захисту автентифікації для автомобільної сигналізації, можна сказати, що відповідно до *моделі супротивника Долева-Яо:*

1) Зловмисник не зможе отримати будь-яке повідомлення, що передане по мережі, так як всі протокольні повідомлення повинні бути захищені шляхом їх шифрування.

2) Зловмисник не може бути авторизованим користувачем мережі через те, що одна або обидві сторони обов'язково повинні підтверджувати свою особистість іншій, забезпечуючи відповідно одностороннюю або взаємну ідентифікацію.

3) Зловмисник не має змоги стати стороною, що приймає повідомлення від будь-якої сторони, що передає або ж посилати будь-якому користувачеві повідомлення від імені будь-якого іншого користувача, так як всі секрети повинні надійно зберігатися в тому числі паролі користувачів, що встановлюють з'єднання між собою.

До того ж відповідно до *моделі знань супротивника Долева-Яо:*

4) Контролюючи засоби зв'язку, зловмисник не може отримати доступ до закритих, внутрішніх ресурсів, наприклад, до пам'яті і жорсткого диска користувача, так як сервер знає якомога менше інформації про систему.

5) Зловмисник не може знайти таємний ключ, знаючи лише відкритий ключ (в криптосистемі з відкритим ключем), так як авторизовані користувачі не мають права розкривати секретні дані.

6) Зловмисник не може розшифровувати, не маючи ключа, або коректно зашифровувати повідомлення за умови використання деякого ідеального алгоритму шифрування, так як повідомлення повинні бути захищені шляхом їх шифрування.