**Лабораторна робота № 1.4.**

**Лабораторна робота №4. Асиметричні криптосистеми**

**Мета роботи.**Освоїти  основні  принципи  роботи  з пакетами програм PGP, PGPfone.

**Хід роботи**

PGP – досить проста у використанні програма, хоча реалiзує надзвичайно складні математичні алгоритми шифрування даних.

Розглянемо роботу програми.

-       Start (Пуск) > Programs (Програми) > PGP > PGP/keys.

-       Вказати власне ім’я ( Full name ) і адресу електронної пошти ( Email address ), не забуваючи, що саме ці дані будуть асоційовані програмою з вашими ключами.

-              Вибір типу ключа (Key Pair Type): ключ RSA архаїчніший і повільніший від Diffie – Hellman/DSS, однак, якщо серед ваших кореспондентів є користувачі більш ранніх версій, ніж PGP 5.0, доведеться використовувати ключ RSA.

-       Вибір довжини загального ключа (Key Pair Size): по замовчуванню (при використанні метода Diffie – Hellman/DSS) пропонується вибрати 2048 – розрядний ключ.

-       Встановити термін, до якого певні ключі можуть використовуватись.

-       Формується додатковий ключ для розшифровування даних (Additional Decryption Key). Він належить до так званих "рятівних ключів" (Recovery Keys), необхідних для відновлення зашифрованих даних у випадку втрати особистого ключа.

-       Генерацiя корпоративного ключа (Corporate Signing Key), яким буде користуватись адміністратор вашого сервера для автоматичного підпису і встановлення довіри стосовно ваших повідомлень.

-       Для адміністратора також формується ключ для апулювання ключа користувача (Designated Revocation Key).

-       Створюємо ключову фразу (passphrase), в якій має бути не менше 8 символів. Можна використовувати будь – які регістри, спеціальні символи, пробіли, будь – яку мову. Якщо подобається набір наосліп, заберіть позначку "Приховати надруковане" (Hide Typing), і тоді текст не відображатиметься.

-       До чергового натискання кнопки "Далі" (Next) доведеться почекати: процедура генерації  ключів може тривати кілька хвилин.

-       Коли ключі згенеровані, треба ввійти в Internet і відіслати відкритий ключ на сервер, де вже складені ключі інших користувачів програми.

Програма PGP потребує відповідального підходу, тому вікно "PGPkeys" вдається закрити не відразу.

Можна діяти інакше: занести свій відкритий ключ на деякий сервер і в підпису свого листа вказати його адресу.

Остання комбінація <Ox5DC10B44> – це ідентифікатор вашого ключа. Він записаний в розділі Key Properties (у вікні PGPkeys після правого кліку мишкою на нашому рядку вибрати Key Properties), у вікні ID в розділі General.

Для того щоб підписати свій ключ, після правого кліку на особистому рядку виберіть меню Sign. Відкриється вікно POP Sign Key з необхідним вам рядком. Після натискання на ОК в новому вікні вкажіть вашу ключову фразу. Наступний клік на ОК, і ключ підписано.

**PGPkeys.** Вибравши цей рядок, ви маєте доступ до таблиці ваших особистих і загальних ключів, а також відкритих ключів ваших кореспондентів. Якщо ваші ключі не згенеровані, виберіть PGPkeys і створюйте їх.

Верхній рядок меню в таблиці PGPkeys надає додаткові можливості. Наприклад, можна додати нові пункти в опис ключів (View):

* ідентифікатор ключа (Key ID),
* рівень довіри,
* дату створення (Creation Date),
* дату знищення (Expiration Date),
* асоційованість з додатковим ключем (ADK).

**PGPtools.**Активізує таблицю інструментів PGP.

Отже, програма РGР інстальована, пара ключів згенерована, відкритий ключ відіслано. Коли прийде відповідь на ваше послання, яка містить відкритий ключ абонента, виділяємо мишкою відкритий блок від BEGIN PGP до END PGP, запам’ятовуємо його в буфері, клікаєм на іконку з замочком, вибираємо Add Key from Clipboard і натискаемо на Import. Ми одержали відкритий ключ. Маючи від абонента зашифроване повідомлення або файл, ви розшифровуєте його через буфер обміну (Decrypt & Verify) або після правого клікання на файлі.

**PGPfone (Pretty Good Privacy Phone)** – програма, яка дає змогу перетворити комп’ютер чи ноутбук у секретний телефон. Програма використовує компресію аудіоданих і потужні криптографічні протоколи, дає можливість безпечно проводити розмови в режимі реального часу. PGPfone приймає голос, використовуючи мікрофон, оцифровує та шифрує сигнал і передає його через модем на інший комп’ютер, на якому також працює програма PGPfone. Всі криптографічні та компресійні протоколи працюють швидко і непомітно, забезпечуючи при тому простий користувальний інтерфейс; передбачена робота з модемом та в мережі Internet.

Зашифрована інформація передається в діапазоні 4410 – 11025 Гц. Під час шифрування голосової інформації є можливість вибору трьох алгоритмів шифрування (Cast, Blowfish, та потрійний DES ) та їх комбінацій. Також користувачу надана можливість вибору величини ключа для шифрування (768 – 4096 біт). Схема з’єднання двох користувачів є простою: один із співрозмовників робить дзвінок, а інший приймає виклик.

Вимоги до конфігурації ПК для нормальної роботи PGPfone:

–      мультимедійний ПК з ОС типу Windows;

–      процесор – не нижче  486; 66 МГц (Pentium рекомендовано);

–      звукова карта, мікрофон, акустична система або навушники.

Перед запуском програми потрібно перевірити мікрофон та навушники (це можна зробити, використовуючи стандартні Windows – програми типу "Звукозапис"). Після перевірки потрібно запустити PGPfone, вибрати тип з’єднання (Internet, modem) та встановити зв’язок, увівши у відповідне поле IP – адресу (якщо тип з’єднання – Internet). Окрім цього можна вибрати ступінь компресії, алгоритм шифрування (CAST, Blowfish, TripleDES, жодний), ступінь шифрування. Залежно від вибраних параметрів змінюватиметься якість зв’язку (зі збільшенням значення частоти дискретизації якість сигналу покращується) та час затримки (залежить від вибраного алгоритму та ступеня криптування).