Автори: Шпортько О. В., Сущук О. А.,

Лабораторна робота № 10.

Тема. Застосування криптографічних засобів захисту інформації. Формування пар відкритих та закритих ключів для реалізації асиметричного шифрування.

Мета. Формування вмінь і навиків організації криптографічного захисту інформації. Отримання знань методів і способів асиметричного шифрування та навиків використання відповідного програмного забезпечення. Закріплення знань файлової структури, вмінь і навиків використання можливостей диспетчерів файлів та поштових систем для пересилання фалів іншим користувачам.

Теоретичні відомості

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, які можуть бути реалізовані за допомогою обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування як Twofish, IDEA, RC4, DEC, та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозумілий набір знаків (тобто, шифротекст). Дешифрування — це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, так і, в кожному випадку, ключем. Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для однозначного шифрування/дешифрування повідомлень. Ключі дуже важливі, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків.

До алгоритмів симетричного шифрування належать способи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або дин ключ легко обчислюється з іншого). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

PGP (англ. Pretty Good Privacy) — комп'ютерна програма, що дозволяє виконувати операції шифрування (кодування) і цифрового підпису повідомлень, файлів і іншої інформації, представленої в електронному вигляді. ЇЇ першу версію розробив Філіп Циммерман у 1991 році.

PGP має безліч реалізацій, сумісних між собою і рядом інших програм (GNUPG, Filecrypt і ін.) завдяки стандарту OPENPGP (RFC 4880), які мають різний набір функціональних можливостей. Існують реалізації PGP для всіх найпоширеніших операційних систем. Окрім вільно поширюваних, є комерційні реалізації.

Користувач PGP створює ключову пару: відкритий і закритий ключ. При генерації ключів задаються їх власник (ім'я і адреса електронної пошти), тип ключа, довжина ключа і термін його дії. PGP підтримує три типи ключів RSA v4, RSA legacy (v3) і Diffiehellman / dss (Elgamal в термінології GNUPG).

Для ключів RSA legacy довжина ключа може складати від 1024 до 2048 біт, а для Diffie-hellman/dss і RS A — від 1024 до 4096. Ключі RSA legacy містять одну ключову пару, а ключі Diffie-hellman/dss і RSA можуть містити один головний ключ і додаткові ключі для шифрування. При цьому ключ електронного підпису в ключах Diffie-hellman/dss завжди має розмір 1024. Термін дії для кожного з типів ключів може бути визначений як необмежений або до конкретної дати. Для захисту ключового контейнера використовується секретна фраза. Ключі RSA legacy (v3) для шифрування зараз не використовуються і виведені із стандарту OPENPGP.

Електронний цифровий підпис формується шляхом підпису дайджеста (хеш-значення) повідомлення (файлу) закритим ключем відправника (автора). Для формування дайджеста можуть використовуватися алгоритми Md5, Sha-1, Ripemd-160, Sha-256, Sha-384, Sha-512. У нових версіях PGP підтримка Md5 здійснюється для збереження сумісності з ранніми версіями. Для підпису використовуються алгоритми RSA або DSA (залежно від типу ключа).

Шифрування здійснюється з використанням одного з п'яти симетричних алгоритмів (AES, Cast5, TRIPLEDES, IDEA, Twofish) на сеансовому ключі. Сеансовий ключ генерується з використанням криптографічного стійкого генератора псевдовипадкових чисел. Сеансовий ключ зашифровується відкритим ключем одержувача з використанням алгоритмів RSA або Elgamal (залежно від типу ключа одержувача).

Для отримання практичних навичок шифрування інформації використаємо саме програму PGP, головна перевага якої – простота використання.

Підготовчий етап заняття. Актуалізація знань

1. Віднайдіть ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту та скопіюйте його в буфер обміну.
2. Створіть нову папку для організації криптографічного захисту та вставте в неї скопійований файл.
3. Для генерації та використання ключів встановіть програму PGP 8.0 (для ОС до Windows XP) чи PDP Desktop 10 (для Windows 7).

Створення пари відкритого і закритого ключів для шифрування повідомлень

4. Для завантаження програми генерації ключів віднайдіть та виберіть у меню **Пуск** операційної системи в групі **PGP** посилання **PGPkeys** для Windows XP (чи **PGP Desktop** для Windows 7).
5. З метою створення власної пари відкритого і закритого ключів оберіть в меню **Keys** для Windows XP (рис. 1) чи в меню **File** для Windows 7 (після активації розділу **PGP Keys** (рис. 2)) пункт **New key**.

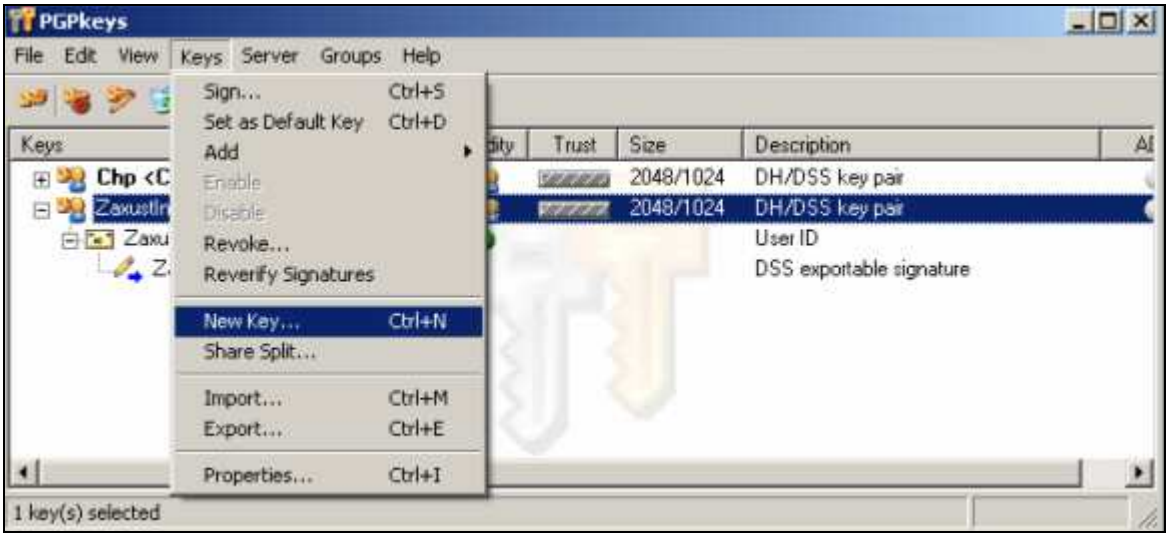

Рис. 1. Меню **Keys** програми адміністрування ключів **PGPkeys**

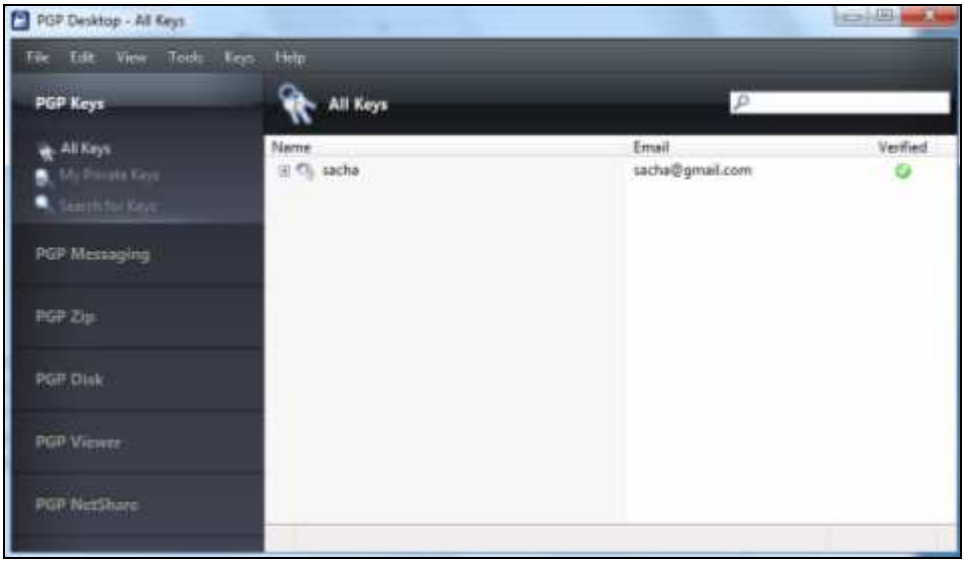

Рис. 2. Розділ **PGP Keys** програми **PGP Desktop**

6. На першому кроці майстра створення ключів введіть латинськими літерами своє прізвище, ім’я та адресу електронної пошти (рис. 3).

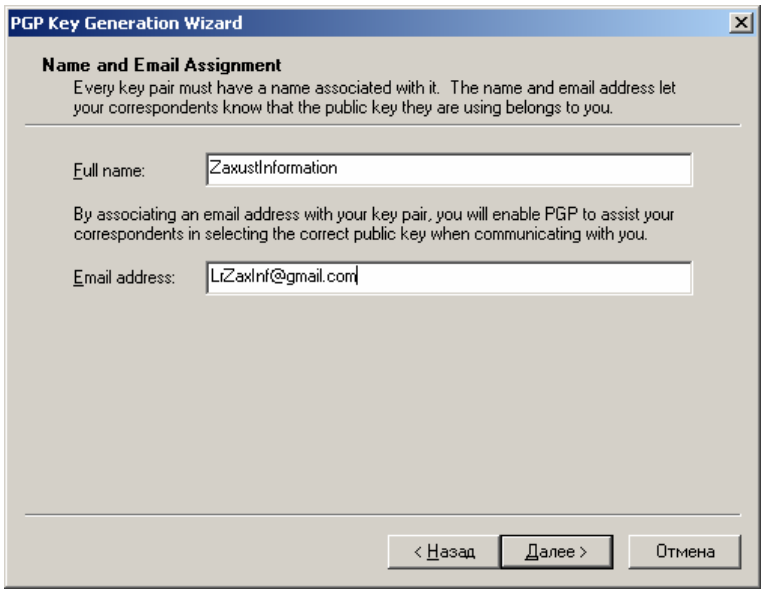

Рис. 3. Вікно першого кроку майстра створення нової пари ключів

7. Для забезпечення використання пари ключів лише вами на другому кроці цього майстра латинськими літерами вкажіть та підтвердіть ключову фразу, знявши попередньо прапорець **Hide Typing** (рис. 4).

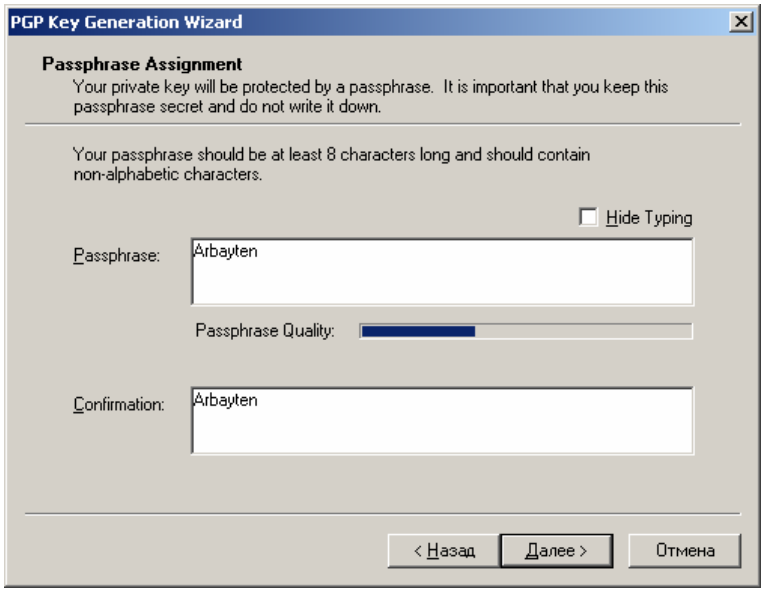

Рис. 4. Вікно другого кроку майстра створення нової пари ключів

8. Самостійно завершіть створення нової пари ключів.
9. Віднайдіть в головному меню програми чи в контекстному меню ключа можливості вибору ключа по замовчуванню та активації/деактивації ключа.

Використання пари відкритого і закритого ключів для передачі зашифрованих повідомлень

10. Використовуючи пункт головного меню програми **Keys** – **Export** (рис. 1) чи **File** – **Export** (рис. 2), створіть файл з вашим відкритим ключем. Перешліть його електронною поштою двом обраним вашим одногрупникам.
11. З метою організації передачі зашифрованих повідомлень вашим одногрупникам перенесіть з отриманих вами листів їх відкриті ключі в папку для організації криптографічного захисту.
12. Використовуючи пункт головного меню програми **Keys** – **Import** (рис. 1) чи **File** – **Import** (рис. 2), перенесіть відкриті ключі одногрупників в програму адміністрування ключів.
13. Для передачі зашифрованих повідомлень одногрупникам, **які надіслали вам свої відкриті ключі**, віднайдіть та виберіть у меню **Пуск** операційної системи посилання **PGPmail** чи активізуйте розділ **PGP Zip** у програмі **PGP Desktop** (рис. 5).

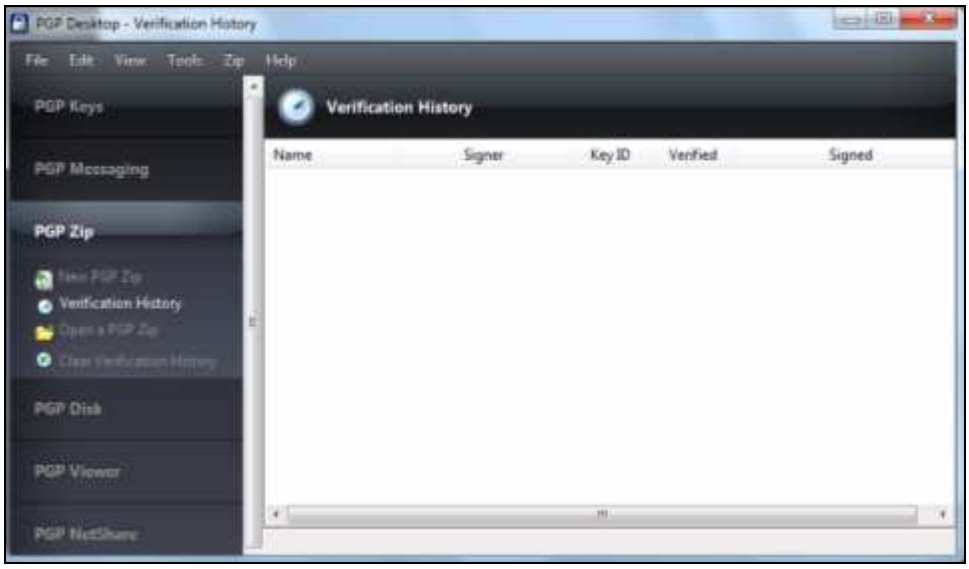

Рис. 5. Розділ **PGP Zip** програми **PGP Desktop**

14. З метою шифрування вашого файлу з описом різновиду апаратного засобу захисту чи зламу захисту для створення зашифрованого файла кожному з вибраних одногрупників послідовно декілька разів виконайте такі дії:
    14.1. В ОС Windows XP натисніть на панелі інструментів програми **PGPmail** (рис. 6) другу кнопку зліва чи в ОС Windows 7 оберіть посилання **New PGP Zip** (рис. 5);

Рис. 6. Панель елементів програми шифрування/розшифровування **PGPmail**

    14.2. На першому кроці завантаженого майстра оберіть файл для шифрування;
    14.3. На другому кроці майстра у вікні вибору ключів шифрування **оберіть відкритий ключ одногрупника, якому бажаєте передати повідомлення** (рис. 7);
    14.4. На наступних кроках майстра введіть назву для зашифрованого файла та самостійно завершіть його створення.

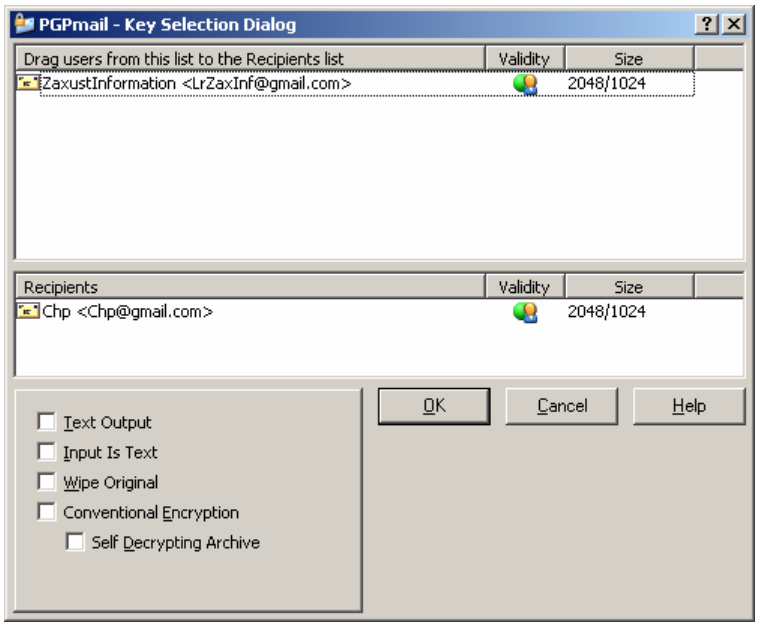

Рис. 7. Вікно вибору ключів шифрування програми **PGPmail**

15. Перешліть електронною поштою зашифровані файли двом обраним вашим одногрупникам, відповідними **відкритими ключами яких ви користувалися для шифрування**.
16. Після отримання від одногрупників файлів, **зашифрованих вашим ключем**, розшифруйте їх, натиснувши в ОС Windows XP на панелі інструментів програми **PGPmail** (рис. 5) п’яту кнопку зліва чи в ОС Windows 7 оберіть в програмі PGP Desktop (рис. 5) посилання **Open a PGP Zip** або аналогічний пункт – у контекстному меню зашифрованого файла.

Завершальний етап заняття. Повторення вивченого матеріалу.

17. Самостійно створіть привітання одногрупнику з нагоди приходу весни, зашифруйте та надішліть його адресату електронною поштою. Розшифруйте надіслані вам привітання.
18. Створіть електронний лист з формулюваннями та відповідями на контрольні запитання у своїй поштовій скриньці на сайті gmail.com. Приєднайте до цього листа архів з наявних у вас відкритих ключів та довільний отриманий зашифрований і відповідний розшифрований документ. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР10_Величко Володимир*. Надішліть створений лист на адресу LRZaxInf@gmail.com.

Контрольні запитання.

1. Чому для шифрування даних на сьогодні крім обраних алгоритмів найчастіше використовуються ключі?
2. Які алгоритми шифрування називаються симетричними, а які – асиметричними, які відкритими, а які – закритими?
3. Яке призначення відкритих ключів?
4. Де і навіщо зберігаються закриті ключі?
5. Як і навіщо використовується ключова фраза, задана при формуванні ключа?
6. Що необхідно встановити і отримати на комп'ютері для стандартизованої передачі зашифрованих повідомлень?
7. Чому розмір зашифрованих файлів може бути меншим від вхідного файла?