Для того, щоб реалізувати визначення координат за методом стереопари, камери повинні розміщуватися так, щоб уявні прямі, які проходять через центри відеокамер, були паралельними між собою. Більше того, нижня границя вертикального кута обзору повинна бути паралельною до земної поверхні, щоб відеокамера захоплювала лише необхідні нам об'єкти, а не витрачала простір кута обзору на відображення не потрібної нам інформації.

Висновок

Обчислення координат видимих об'єктів було реалізовано за методом стереопари. Відносно точності обчислення тривимірних координат та затрат пам'яті і ресурсів процесора алгоритм розміщення камер за методом стереопари має доволі високі показники. Затрати пам'яті для зберігання програми за методом стереопари – 1.92 кбайт. Точність обчислення тривимірних координат становить L – 0,96% * L/100 , де L – відстань між камерою та об'єктом.

1. Андреев В.А.. Разработка первой отечественной системы видеозахвата движения человека // Труды конференции «Новые информационные технологии» (Судак, Крым, 22–29 мая 2005 г.). 2. Pham D.T., Karaboga D., Intelligent Optimisation Techniques, Springer, 2000. – 302 p. 3. Разработка устройства ввода трехмерной информации с использованием средств видеозахвата движения / Компанія "Дериа Графикс". – СПб., 2005. 4. http://dsp-book. narod.ru/dspimage/ chapter6.pdf, Фотограмметрия и стереовидение. 5. http:// www.analog.com/ en/ prod/0,,ADSP-BF535P,00.html.

УДК 681.3

М. Назаркевич, А. Гладець
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

РОЗРОБЛЕННЯ ПРОГРАМНОГО ПАКЕТА ДЛЯ ШИФРУВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ЗАСОБАМИ ATEB-ФУНКЦІЙ

Для шифрування інформації було застосовано алгоритм одноразового блокнота. Для генерації ключів використовувалися Ateb-функції. Стійкість шифруваня забезпечувалася аперіодичністю Ateb-функцій. Розроблено програмний пакет, який реалізує алгоритм одноразового блокнота для шифрування електронних документів.

For enciphering information are used the algorithm of non-permanent notebook. For the generation of the keys are used Ateb-functions. Firmness of enciphering is provided by not periodical of Ateb-functions. The developed program realize the algorithm of non-permanent notebook for enciphering of electronic documents.

Вступ

У процесі розвитку суспільства людство поступово переходить від традиційних форм збереження інформації (паперових документів) і цінних паперів (грошей, векселів) до їхніх електронних аналогів. Саме тому виникає потреба у захисті цих документів від несанкціонованого доступу. Одним із методів, що може забезпечити такий захист, є шифрування документів. Алгоритми шифрування поділяють на симетричні, асиметричні і хеш-функції.

Симетричні криптосистеми — спосіб шифрування, в якому для шифрування і розшифрування застосовується той самий криптографічний ключ [1].

Сьогодні симетричні шифри – це:

• блокові шифри. Обробляють інформацію блоками певної довжини (зазвичай 64, 128 бітів), застосовуючи до блоку ключ у встановленому порядку, як правило, декількома циклами перемішування і підстановки, що називаються раундами.

• потокові шифри, в яких шифрування проводиться над кожним бітом або байтом початкового (відкритого) тексту з використанням гамування.

Порівняно з іншими для симетричних криптосистем характерні такі переваги:

1. Швидкість (за даними Applied Cryptography — на 3 порядки вище);
2. Простота реалізації (за рахунок простіших операцій);
3. Менша необхідна довжина ключа для аналогічної стійкості;
4. Добра вивченість (за рахунок більшого віку).

Але у симетричних криптосистем є і недоліки, а саме:

1. Складність управління ключами у великій мережі;
2. Складність обміну ключами.

До асиметричних криптосистем належить криптографічна система з відкритим ключем. Це система шифрування або електронного цифрового підпису, при якому відкритий ключ передається по відкритому каналу і використовується для перевірки електронного цифрового підпису і для шифрування повідомлення [2]. Для генерації електронного цифрового підпису і для розшифрування повідомлення використовується секретний ключ.

Перевага асиметричних шифрів перед симетричними шифрами полягає у відсутності необхідності попередньої передачі секретного ключа по надійному каналу.

Серед недоліків криптосистем з відкритим ключем можна навести такі [2]:

1. Асиметричні криптосистеми вимагають великих обчислювальних ресурсів, тому на практиці використовуються поєднано з іншими алгоритмами.

2. Для ЕЦП повідомлення заздалегідь піддається хешуванню, а за допомогою асиметричного ключа підписується лише відносно невеликий результат хеш-функції.

3. Для шифрування вони використовуються у формі гібридних криптосистем, де великі обсяги даних шифруються симетричним шифром на сеансовому ключі, а за допомогою асиметричного шифру передається тільки сам сеансовий ключ.

Крім вищевикладених алгоритмів шифрування, широке застосування отримали хеш-функції, які засновані на концепції односторонніх математичних функцій. Суть цього підходу полягає у тому, що, маючи функцію f() і повідомлення m, можна доволі просто отримати перетворення f(m). Водночас, маючи функцію f() і результат перетворення f(m), обчислити початкове повідомлення m є практично неможливим.

На відміну від методів шифрування, які забезпечують конфіденційність даних, хеш-функції використовуються переважно для перевірки цілісності і автентичності інформації.

Основними характеристиками хеш-функцій є:

• хеш-функція повинна забезпечувати стиснення вхідної інформації;

• обчислення початкового повідомлення m неможливе навіть за наявності хеш-функції h() і результату перетворення повідомлення h(m);

• якщо повідомлення m, хеш-функція h(), результат перетворення h(m), неможливе існування виразу h(m)= h(m'), де деяке повідомлення m' не дорівнює m ($m' \neq m$);

• за наявності хеш-функції h() і умови $m' \neq m$ практично неможливо обчислити h(m)= h(m').

Хеш-функції також можуть будуватися на основі ключа. Ключем переважно є послідовність випадкових символів, які, як правило, зберігаються в секреті.

Сучасна криптографія характеризується використанням відкритих алгоритмів шифрування із застосуванням обчислювальних засобів. Відомо більше десятка перевірених алгоритмів шифрування, які при використання ключа достатньої довжини і коректної реалізації алгоритму криптографічно стійкі.

Алгоритм шифрування електронної інформації засобами Ateb-функцій

Для розв'язання поставленої задачі було використано алгоритм шифру одноразового блокноту, розроблений Гілбертом Вернамом [1]. Перед шифруванням повідомлення *M* записують у двійковій формі. Ключем *K* є довільне двійкове слово однакової з *M* довжини. Криптотекст *C* отримують побітовим додаванням повідомлення і ключа, тобто

$$C = M \oplus K.$$

Дешифрування у шифрі одноразового блокноту збігається із шифруванням – щоб отримати вихідне повідомлення *M*, треба додати до криптотексту *C* той самий ключ *K*. Це легко обґрунтувати:

оскільки $C = M \oplus K$, то $C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M$.

Ключ *K* – це протабульоване значення асиметричної Ateb-функції $sha(n, m, \omega)$ у цілочисловому вигляді, що залежить від параметрів *n, m* [3].

Шеннон довів, що шифр одноразового блокнота при певних властивостях ключа є абсолютно надійним або, як ще кажуть, надійним у теоретико-інформаційному сенсі. Якщо суперник не знає ключа *K*, то з підслуханого криптотексту *C* він зовсім нічого не може довідатись про повідомлення *M*. Справді, двійкове слово *C* могло би бути криптотекстом для будь-якого повідомлення *M'*, якби шифрування здійснювалось з деяким іншим ключем *K'*, а саме $K' = M' \oplus C$, тоді як для суперника всі ключі однаково ймовірні[1].

Алгоритмом одноразового блокнота передбачено такі вимоги до ключа:

- Довжина шифрувальної гами повинна бути не меншою за довжину повідомлення, що захищається.
- Для кожного повідомлення необхідно використовувати новий ключ (повторне використання ключа є неприпустимим).

Формат PostScript файла

Формати PostScript (PS) чи Portable Document Format (PDF) сьогодні стали стандартами у видавничій справі. Інформація, записана у цих форматах, забезпечує можливість обміну і проглядання цифрових документів без обов'язкової прив'язки до програмних засобів, в яких вони створені. PostScript – мова для керування вивідними пристроями, такими, як лазерні принтери. Ця мова має кілька переваг:

- PostScript – машинно-незалежна мова. Це означає, що PostScript-файл може бути виведений на будь-якому PostScript-пристрої.
- Синтаксис PostScript є доступний користувачам.
- Покращена підтримка кольороподілу.
- Підтримка PDF-формату.
- Web- друкування інформації.

Структура PostScript документа зображена на рис. 1 і складається з двох частин: прологу та сценарію.

Пролог – це набір певних процедур, які потрібно оголосити і які потім виконуються у сценарії. Це перша частина будь-якого електронного PS-документа.

Сценарій – друга частина будь-якого електронного документа, яка генерується автоматично прикладною програмою, вже описаною в пролозі.

Сценарій складається з процедур. Сценарій, на відміну від прологу, зазвичай відтворюється у традиційному стилі, повторюється і є простим.

Файли складаються з певних частин з маркерами, які вказують на початок певної секції нових даних. У секції розміщено сам текст у шістнадцятковому форматі [4] Під час шифрування відкритий текст заміщується зашифрованим текстом, при цьому структура файла не порушується. Отже, є однозначна можливість зашифрувати будь-який документ.

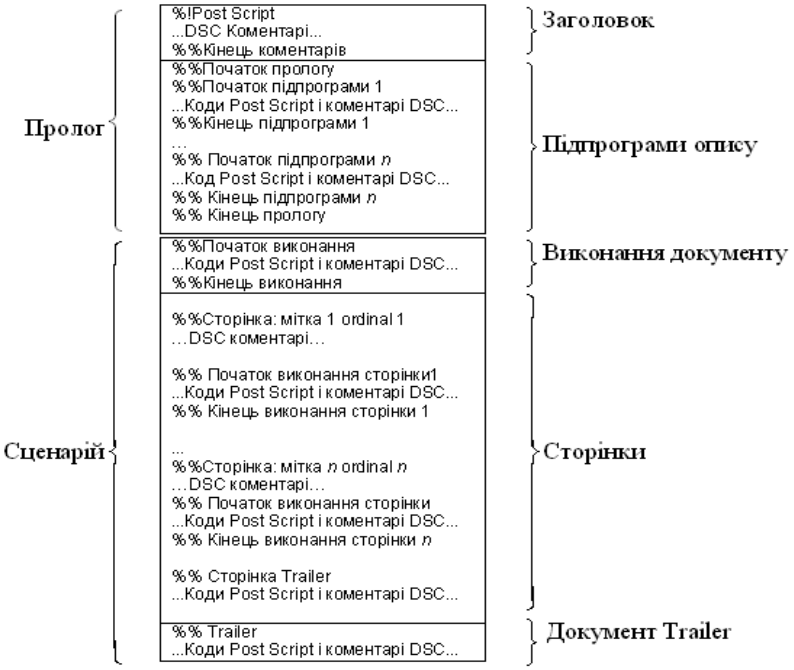


Рис. 1. Структура PostScript документа

Рис. 2. Алгоритм роботи програмного пакета

Опис програмного пакета

Програмний пакет складається з чотирьох частин:

1. Модуль генерації ключів із використанням Ateb-функцій.
2. Модуль пошуку текстових рядків у PostScript документі.
3. Модуль пошуку у зчитаному рядку тексту та його шифрування.
4. Запис зашифрованого тексту у файл.

Програма реалізовує алгоритм, зображений на рис. 2.

Програма містить меню налаштувань генератора ключів і параметрів Ateb- функцій (рис. 3), а саме: параметрів *m*, *n*, від яких безпосередньо залежить генератор ключів, крок ітерацій, точність обчислень, діапазон значень аргументу Ateb-функцій та кількість проміжків на які розбивається цей діапазон. Для шифрування необхідно вказати шлях до потрібного файла і задати параметри шифрування (рис. 4).

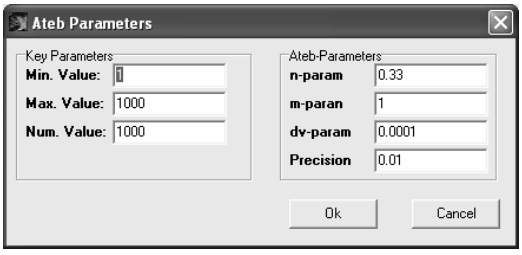


Рис. 3. Меню налаштування параметрів програми

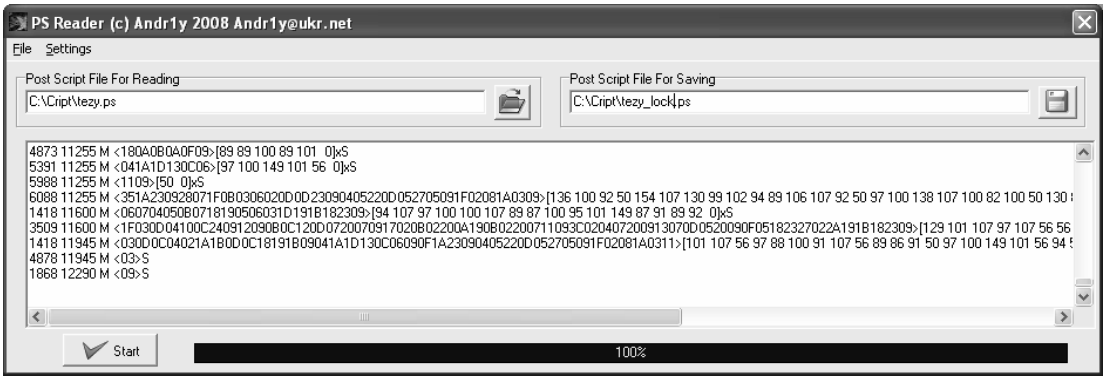
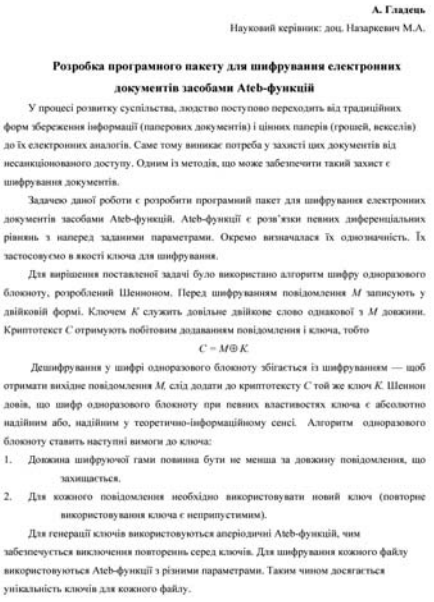


Рис. 4. Головне вікно програми



А. Гладень

Науковий керівник: доц. Назаркевич М.А.

Розробка програмного пакету для шифрування електронних документів засобами Ateb-функцій

У процесі розвитку суспільства, людство поступово переходить від традиційних форм збереження інформації (паперових документів) і цінних паперів (грошей, векселів) до їх електронних аналогів. Саме тому виникає потреба у захисті цих документів від несанкціонованого доступу. Одним із методів, що може забезпечити такий захист є шифрування документів.

Задачею даної роботи є розробити програмний пакет для шифрування електронних документів засобами Ateb-функцій. Ateb-функції є розв'язки певних диференціальних рівнянь з наперед заданими параметрами. Окремо визначалася їх однозначність. Їх застосовуємо в якості ключа для шифрування.

Для вирішення поставленої задачі було використано алгоритм шифру одноразового блокноту, розроблений Шенноном. Перед шифруванням повідомлення *M* записують у двійковій формі. Ключем *K* служить довільне двійкове слово однакової з *M* довжини. Криптотекст *C* отримують побітовим додаванням повідомлення і ключа, тобто

$$C = M \oplus K.$$

Дешифрування у шифрі одноразового блокноту збігається із шифруванням — щоб отримати вихідне повідомлення *M*, слід додати до криптотексту *C* той же ключ *K*. Шеннон довів, що шифр одноразового блокноту при певних властивостях ключа є абсолютно надійним або, надійним у теоретично-інформаційному сенсі. Алгоритм одноразового блокноту ставить наступні вимоги до ключа:

1. Довжина шифруючої гами повинна бути не менша за довжину повідомлення, що захищається.
2. Для кожного повідомлення необхідно використовувати новий ключ (повторне використовування ключа є неприпустимим).

Для генерації ключів використовуються аперіодичні Ateb-функцій, чим забезпечується виключення повторень серед ключів. Для шифрування кожного файлу використовуються Ateb-функції з різними параметрами. Таким чином досягається унікальність ключів для кожного файлу.

Рис. 5. Документ до шифрування

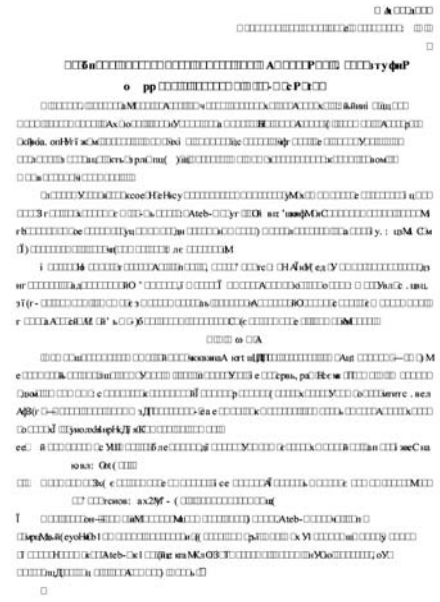


Рис. 6. документ після шифрування з параметрами ateb- функції n=1/3, m=1

Результати роботи програми

Приклад вихідного документа наведено на рис. 5, а на рис. 6 – документ після шифрування. Шифрування проводилися за допомогою $sha(n,m,\omega)$ з параметрами n=1/3, m=1, $\omega \in [0{,}1000]$. Фрагменти програми наведені на рис. 7, 8.

При дешифруванні вказується шлях до зашифрованого файла і параметри, при яких файл був зашифрований.

```
dup 33 /afii10096 put
pop
4889 3308 M <13210l191A0D02>[100 149 102 89 87 94  0]xS
5610 3308 M <051D0219>[107 107 100  0]xS
6013 3308 M <1A181D02OD02051DOCOAOC1EO2O1>[86 102 107 100 94 100 106 107 89 100
89 100 100  0]xS
7395 3308 M <OE>S
7502 3308 M <1A14O5OD15O1051AOAO8O1OEO31517160E1EO5>[87 91 107 94 56 102 107 87
100 89 102 106 107 56 107 107 107 100  0]xS
1991 VM?
```

Рис. 7. Частина PostScript документа до шифрування

```
dup 33 /afii10096 put
pop
4889 3308 M <888EC5COF5OA1F>[100 149 102 89 87 94  0]xS
5610 3308 M <30516664>[107 107 100  0]xS
6013 3308 M <8CA8D7E7OC1F3C4B7F9AA2D3EEOC>[86 102 107 100 94 100 106 107 89 100
89 100 100  0]xS
7395 3308 M <23>S
7502 3308 M <577A95BFC1F6195A6E81AEDBF8365C6495DAE8>[87 91 107 94 56 102 107 87
100 89 102 106 107 56 107 107 107 100  0]xS
1991 VM?
```

Рис. 8. Частина PostScript документа після шифрування

Висновки

Було розроблено програму для реалізації описаного алгоритму шифрування. Для генерації ключів використовували аперіодичні Ateb-функції. Цим запобігають повторенням серед ключів, а отже, забезпечують стійкість алгоритму. Для шифрування кожного файла використовували Ateb-функції з різними параметрами. Так досягнуто унікальності ключів для кожного файла.

1. Вербицький О.В. Введення в криптологію. – Львів: Наук.-техн. літ., 1998. – 248 с. 2. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 320 с. 3. Грицик В.В., Назаркевич М.А. Алгоритм табулювання Ateb-функцій // Системні технології: Регіональний міжвузівський збірник наукових праць. – Дніпропетровськ, 2006. – Вип. № 6(47). – С. 77–83. 4. PostScript language reference manual / Adobe Systems Incorporated.