набагато швидше виявити і повторно передати втрачений пакет, ніж Tahoe; не повинен чекати 3-х подвійних АСК і тому він може швидше повторно передати втрачений пакет, ніж Reno і NewReno; завдяки зміненим алгоритмам *Запобігання перевантаженню* і *Повільного старту* здійснює менше повторних передач, що призводить до ефективнішого використання ресурсів мережі, ніж NewReno і Tahoe; при оцінюванні перевантаження вимірює пропускну здатність і змінює її замість втрати пакета, що дає краще використання смуги пропускання і менше перевантажень, чим в Tahoe і SACK; вирівнює свою норму посилки пакетів до одержувача в оптимальній смузі пропускання, тобто спричиняє стабільність, на відміну від SACK.

1. Leland W.E., Taqqu M.S., Willinger W., Wilson D.V. On the self-similarnature of ethernet traffic, IEEE/ACM Transactions of Networking, vol. 2(1). – pp. 1–15, 1994. 2. Столлингс В. Современные компьютерные сети. – СПб.: Питер, 2003. – С. 783. 3. Kirichenko L., Radivilova T., Karpukhin O. Improvement quality of network service under selfsimilar loading, Стратегия качества в промышленности и образовании // Мат-лы 4-й междунар. конф. – Варна, 2008. – С. 612–615. 4. Floyd S., Jacobson V. Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, August 1993. – Vol. 1(4). – pp. 397–413, 5. Fall K., Floyd S. Simulation-based comparison of tahoe, reno, and sack tcp, Computer Communication Review, 2002. – Vol. 26. – pp. 5–21.

УДК 621.395

В. Хома
Національний університет “Львівська політехніка”,
кафедра захисту інформації,
Політехніка Опольська, інститут автоматики і інформатики

ОПИС І ХАРАКТЕРИСТИКА КРИПТОЛОГІЧНОГО ПАКЕТА CRYPTOOL ЯК НАВЧАЛЬНОГО ІНСТРУМЕНТА

Репрезентовано вільно поширюваний криптологічний пакет CrypTool. Описано функціональні можливості цього програмного пакета, набір алгоритмів шифрування та цифрового підпису, а також інструментів їхнього криптоаналізу. Наведено оцінку застосування криптологічного пакета CrypTool у навчльному процесі.

Ключові слова: крипто логічний, програмний, крипто аналіз, цифровий підпис.

The free distribute cryptology package of CrypTool is presented in the article. Functional possibilities of this programm package, set of encryption and digital signature algorithms and also instruments of their cryptoanalysis are described. Application of cryptology package of CrypTool in an educational process is estimated.

Keywords:

1. Вступ. Історія створення та розвитку криптопакета

CrypTool – це вільно поширюваний криптологічний програмний пакет. У ньому заімплементовано багато криптографічних алгоритмів та протоколів як класичної, так і асиметричної криптографії, а також засоби криптоаналізу [1–3]. Пакет CrypTool є надзвичайно потрібним і корисним інструментом для вивчення й аналізу криптографічних перетворень, а також висвітлення реальних загроз під час практичного застосування криптографічних засобів у сучасних інформаційних системах.

Проект CrypTool започаткував професор Бернхард Есслінгер (Esslinger) у 1998 році, тоді ж розвивається на засадах відкритого програмного забезпечення такими німецькими університетами,

як Зіген (Siegen) і Дармштат (Darmstadt). На момент публікування статті стабільною була версія програми CrypTool 1.4.30, написана мовою C++ , яка працює лише під операційною системою Microsoft Windows. Проводиться робота із перенесення програми на інші платформи, такі як Linux чи Mac. У 2007 році стартували два проекти, що мають на меті підготовку програми з використанням гнучкої архітектури «підключи і працюй»: проект CrypTool 2.0 використовує C#/.NET/WPF, натомість проект CrypTool 1.0 спирається на платформу Java/Eclipse/RCP/SWT [5].

CrypTool відзначений багатьма нагородами у категорії навчального програмного забезпечення, зокрема TeleTrusT Special Award (2004), EISA (2004), IT Security Award NRW (2004), Selected Landmark in the Land of Ideas (2008).

2. Функціональність пакета CrypTool та опис інтерфейсу

У програмному пакеті CrypTool реалізовано практично всі сучасні криптологічні функції, завдяки чому в одному середовищі можна вивчати не лише суть та особливості різних криптографічних алгоритмів, але також загрози та ризики, які можуть виникати при застосуванні криптографічних засобів захисту.

Пакет CrypTool оснащений зручним інтуїтивно зрозумілим графічним інтерфейсом користувача. Головне вікно програми (див. рис.1) містить 10 меню, де, крім традиційних для аплікацій системи Windows рубрик **File, Edit, View, Window, Help,** розміщено такі спеціалізовані засоби пакета, як **Crypt/Decrypt (Шифрування/Дешифрування), Digital Sygnatures/PKI (Цифрові підписи/ІПК, Indiv. Procedures (Окремі Процедури), Analysis (Криптоаналіз), Options (Опції)**.

Структура меню та підменю в програмі CrypTool генерується динамічно залежно від виконуваних дій та типу документа (бінарний чи текстовий). Всі позиції меню завжди видимі, але можна вибрати лише ті, для яких така операція має сенс. Доступними для криптографічних перетворень є дані, які знаходяться у так званому «активному» вікні.

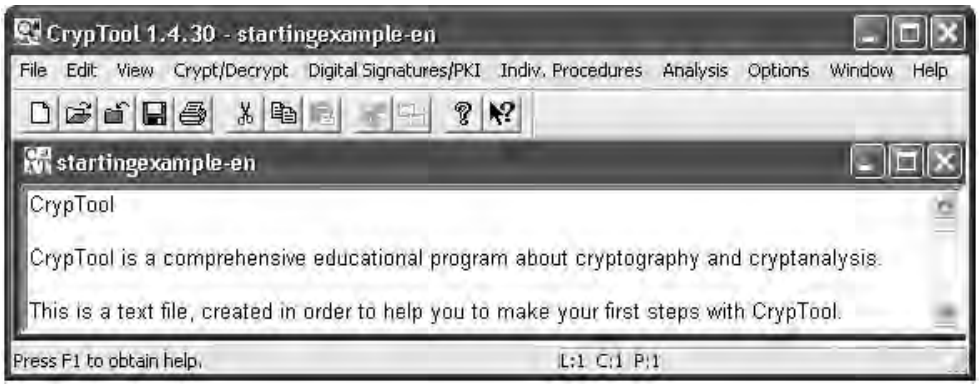

Рис.1. Вигляд головного вікна програми CrypTool

Меню **Crypt/Decrypt** містить засоби дослідження найвідоміших історичних шифрів, найпопулярніших сучасних симетричних блокових алгоритмів (DES, IDEA, AES та ін.) і асиметричних – RSA [2, 3, 4]. Разом з тим частину реалізацій криптоалгоритмів автори розмістили у меню **Indiv. Procedures.** Це зокрема стосується алгоритму Diffie-Hellman – першого алгоритму асиметричної криптографії. У цьому меню доступними також є засоби анімації таких алгоритмів шифрування, як Caesar, Vigenere, Nihilist, DES, які дозволяють покрокове дослідження криптографічних перетворень і можливість архівування послідовності цих даних у файлі AML. Можливий також режим автоматичного перегляду анімації загалом із регульованою тривалістю окремих кроків. Анімацію алгоритмів здійснюється за допомогою безкоштовного програмного забезпечення ANIMAL, що є додатком Java.

Цікавою є візуалізація роботи роторної шифрувальної машини Enigma, яка у першій половині XX століття була неперевершеним досягненням криптографії, а також найновішого міжнародного стандарту XXI століття алгоритму AES. На рис. 2. наведено вигляд вікна візуалізації роботи роторної шифрувальної машини Enigma.

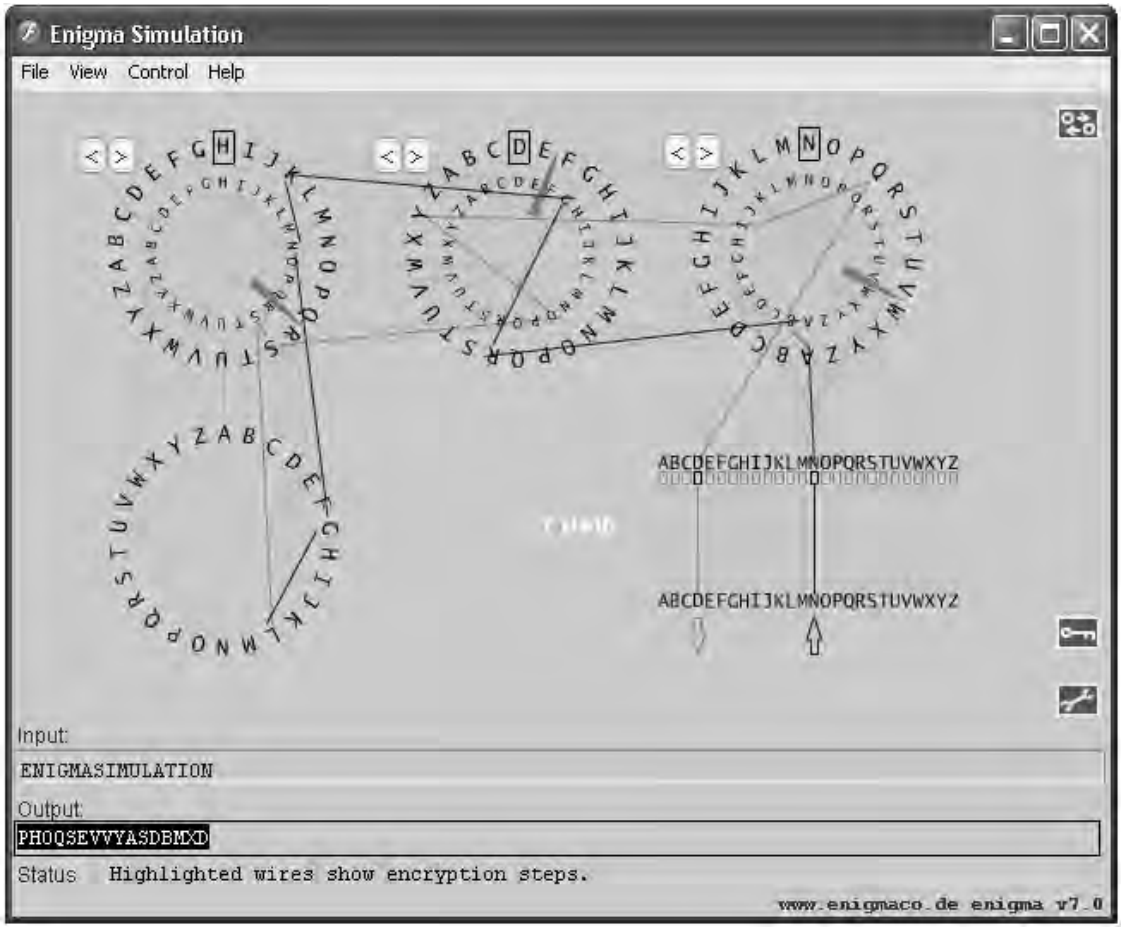

Рис. 2. Вигляд вікна візуалізації роботи роторної шифрувальної машини Enigma

В меню **Digital Sygnatures/PKI** входять засоби, що дають змогу ознайомитися із технологією створення та верифікації цифрового підпису, а також генерування, зберігання та висвітлення параметрів публічних і приватних ключів асиметричної криптографії (алгоритмів RSA, DSA і на еліптичних кривих).

Меню **Indiv. Procedures** є найскладнішим як за тематикою розміщених засобів, так і за деревом підменю. Тут, крім вже згаданих засобів візуалізації окремих алгоритмів шифрування, розміщено набір програм для обчислення хеш-функцій, засоби кодування і стиснення даних, формування випадкових послідовностей та оцінювання якості паролю. Для зручності в окремому підменю зібрано засоби, що стосуються найпопулярнішого асиметричного алгоритму RSA – генерування простих чисел, тестування чисел на предмет простоти, факторизація чисел, а також демонстрування RSA у режимі шифрування/дешифрування і цифрового підпису.

В меню **Analysis** є засоби, що уможливлюють проведення автоматичного криптоаналізу історичних шифрів, сучасних симетричних блокових і асиметричних шифрів, а також хеш-функцій. У ручному режимі користувач може вибрати окремий метод для самостійного криптоаналізу.

В меню **Options** можна задавати набір засобів для автоматичного криптоаналізу історичних та сучасних шифрів, а також допустимий набір знаків текстових документів (великі літери, малі літери, цифри, знаки пунктуації, пробіл). Всі алгоритми в пакеті CrypTool реалізовані за міжнародними стандартами і нормами.

У програмі CrypTool велику увагу приділено наданню доступної допомоги для кожної із опцій програми. За потреби користувач, натиснувши клавішу **F1**, зможе пошукати ширший опис окремих алгоритмів.

У файлах допомоги знаходиться:

- пояснення всіх основних криптографічних термінів;

- короткий перелік посилань на джерела, що допоможуть поглибити знання із відповідного питання;
- огляд історії криптології та характеристика тенденцій її подальшого розвитку;
- готові приклади, які полегшують та прискорюють процес вивчення алгоритмів;
- добре систематизовані теми із криптології.

3. Шифрування і дешифрування

Для дослідження процесів шифрування/дешифрування в програмі CrypTool передбачено меню **Crypt/Decrypt,** що містить такі підменю:

Symmetric (classic) – історичні шифри;

Symmetric (modern) – сучасні симетричні алгоритми;

Asymmetric – асиметричні алгоритми;

Hybrid – гібридні криптосистеми.

Реалізовані в підменю **Symmetric (classic)** історичні шифри охоплюють чотири класи шифрів заміни:

1. Одноалфавітні (**Caesar/Rot-13, Substitution/Atbash**)
2. Багатоалфавітні (**Vigenere, Vernam, XOR, Solitaire, Byte Addition**)
3. Поліграмні (**Playfair, Hill**)
4. Гомоморфні **(Homophone**)

Крім того, у цьому ж підменю представлені також шифри перестановок **Scytale/Rail Fence, Permutation/Transposition** та комбіновані (заміна і перестановка) шифри (**ADFGVX**).

В підменю **Symmetric (modern)** представлені такі сучасні симетричні блокові алгоритми як **IDEA, RC2, RC4, DES, Triple DES, AES (Rijndael)**, а у підменю **Further Algorithms** також алгоритми-фіналісти міжнародного конкурсу Advanced Encription Standart – **MARS, RC6, Serpent, Twofish**. У розширеному переліку доступних алгоритмів також є модифікований DES – **DESX, DESL, DESXL.** При цьому алгоритми DES, Triple DES можуть працювати не лише у режимі електронної кодової книжки (**Electronic Code Book – ECB**), але і у режимі зв'язування блоків шифрограми (**Ciphertext Block Chaining – CBC**). Цікавою є можливість шифрування/ дешифрування файлів алгоритмом AES в режимі саморозпаковування, що дозволяє розшифровувати файли поза середовищем програми CrypTool.

В підменю **Asymmetric** доступні три директиви: **RSA Encryption, RSA Decryption, RSA Demonstration**. Перші дві директиви призначені відповідно для шифрування і дешифрування даних з використанням публічного і приватного ключів RSA заздалегідь створених в меню **Digital Sygnatures/PKI>PKI>Generate/Import Keys**. Є можливість визначати тривалість процесів шифрування і дешифрування. Дешифрування вимагає приватного ключа, доступ до якого захищено паролем.

Директива **RSA Demonstration** призначена для дослідження в одному вікні трьох кроків алгоритму: генерування пари ключів, шифрування і дешифрування.

Через підменю **Hybrid** стають доступними директиви **RSA-AES Encryption, RSA-AES Decryption, ECC-AES Encryption, ECC-AES Decryption**, які призначені для покрокового дослідження процесів шифрування і дешифрування у змішаних симетрично-асиметричних системах. Як відомо, у сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, наприклад, AES, а завданням «повільних» асиметричних алгоритмів є шифрування ключа сесії.

Окрім алгоритму RSA в змішаній криптосистемі використовується також криптографія на еліптичних кривих (Elliptic Curves – ECC) [2, 3].

4. Автентифікація даних. Цифровий підпис

Важливим для практики завданням асиметричної криптографії є забезпечення цілісності та автентичності даних без їх шифрування. Загальновизнаним сьогодні підходом щодо реалізації цього завдання є технологія цифрового підпису [3, 4].

В меню **Digital Sygnatures/PKI** доступні директиви створення цифрового підпису **Sign Document**, верифікації цифрового підпису **Verify Document** та виділення цифрового підпису **Extract Document.**

На рис. 3 наведено вигляд вікна директорії **Signature Demonstration (Signature Generation),** яка є зручним інструментом вивчення технології створення та верифікації цифрового підпису.

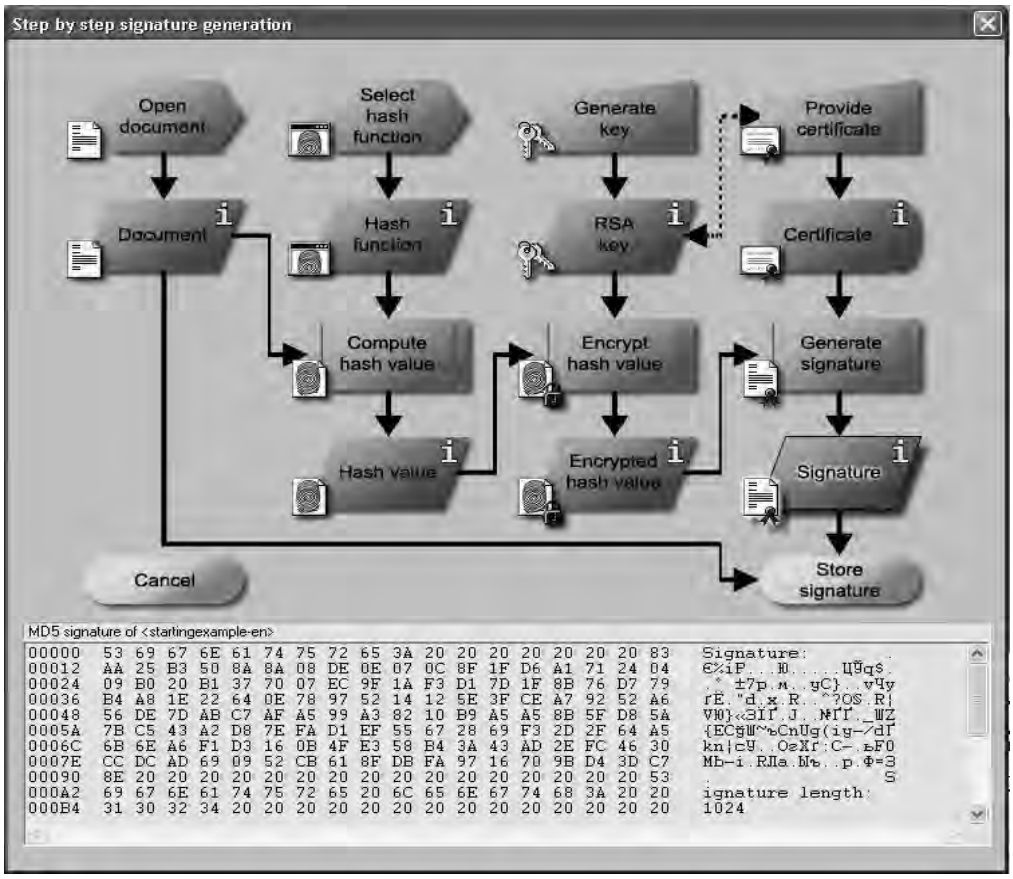

Рис. 3. Вигляд вікна директорії вироблення цифрового підпису

В підменю **PKI** (**Public Key Infrastucture**) доступні дві директиви **Generate/Import Keys** та **Key Display/Export,** які призначені відповідно для генерування/імпорту ключа та висвітлення/експоту ключа. Імпорт чи експорт ключів здійснюється із відповідних файлів. Приватні ключі зберігаються у зашифрованому вигляді, а публічні ключі репрезентуються через цифрові сертифікати (рис. 4).

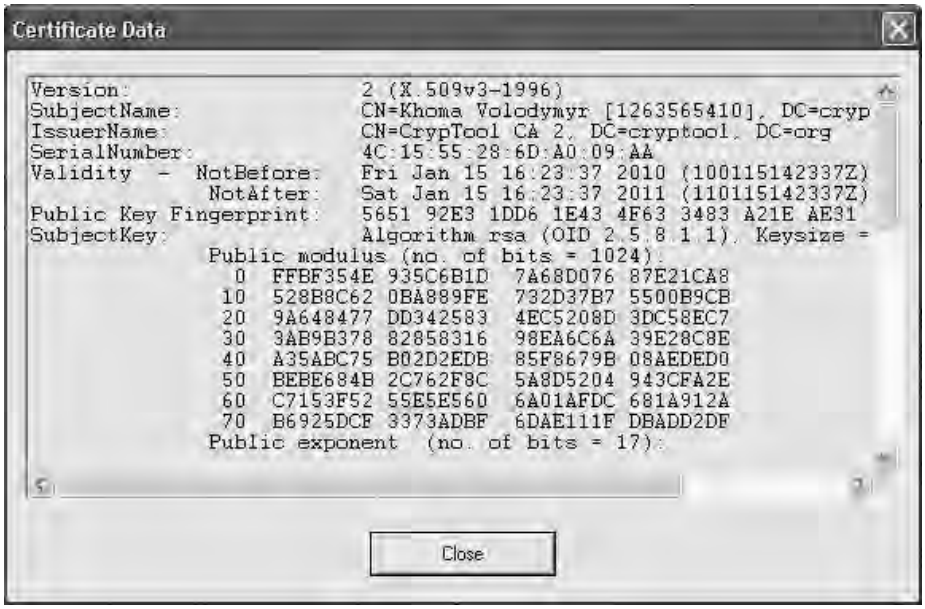

Рис. 4. Вигляд цифрового сертифікату

5. Окремі процедури і алгоритми

У меню **Indiv. Procedures** включено різні процедури і алгоритми, які застосовуються у сучасній криптології. Нижче наведено коротку характеристику найважливіших засобів цього меню.

Підменю **Hash** містить директиви до обчислень значень таких хеш-функцій: **MD2, MD4, MD5, SHA-1, SHA-256, SHA-512, RIPEMD-160**. За допомогою директиви **Hash Demonstration** можна досліджувати властивості хеш-функцій, зокрема випадковість змін їх значень внаслідок редагування тексту та практичну складність знаходження колізії, коли два різні документи дають одне значення хеш. Для цього в інтерактивному режимі користувач редагує оригінальний файл, спостерігаючи зміни у значеннях хеш оригінального і відредагованого файла. Зміни значень хеш інтерпретуються як у побітовому, так і у процентному вимірі.

У підменю **Hash** є ще дві директиви, які ілюструють застосування хеш-функцій для автентифікації повідомлень (**Generation of MACs**) та генерування ключів на основі паролю (**Key Generation from Password**).

Меню **RSA Cryptosystem** містить підменю та директиви із різноманітними інструментами, що дають змогу поглибленого вивчення алгоритму RSA:

- **Prime Number Test** – аналізує числа на предмет простоти за тестами **Miller-Rabin, Fermat, Solovay-Strassen і Agrawal-Kayal-Saxena**;
- **Generate Prime Numbers** – генерує два прості числа **p** і **q** у заданих користувачем діапазонах;
- **Factorization of a Number** – факторизує задане користувачем число на прості множники;
- **RSA Demonstration (**ця функція дублюється, описана раніше у меню **Crypt/Decrypt>Asymmetric)**;
- **Signature Demonstration (Signature Generation) (**ця функція дублюється, описана раніше у меню **Digital Sygnatures/PKI)**;
- **Lattice Based Attacks on RSA (**ця функція дублюється і оскільки належить до криптоаналізу, тому описана нижче в меню **Asymmetric Encryption).**

У підменю **Tools** зосереджені окремі засоби, що мають важливе значення для криптографічного захисту інформації:

- **Codes** – підменю із такими засобами кодування/декодування, як **Base64 Encode/Decode, UU Encode/Decode** і **Decode ASN.1 Code of a Document;**
- **Compress –** підменю із Zip і UnZip;
- **Generate Random Numbers –** директива для генерування псевдовипадкових послідовностей з використанням таких генераторів, як **SECUDE Library random number generator, x^2(modN) random number generator, Linear Congruence Generator** та **Inverse Congruence Generator;**
- **Password Quality Meter –** директива для оцінки якості паролю;
- **Password Entropy –** директива для автоматичного генерування паролю на основі заданої користувачем ентропії та простору символів.

Меню **Indiv. Procedures** крім розглянутих додатково містить такі підменю:

- **Protocols;**
- **Chinese Remainder Theorem Applications;**
- **Visualization of Algorithms;**
- **Secret Sharing Demonstration (Shamir);**
- **Educational Games;**
- **Number Theory – Interactive.**

6. Криптоаналіз

Основним завданням криптоаналізу, як розділу криптології, є об’єктивна оцінка стійкості шифрограм. Сьогодні в практичній криптографії використовуються алгоритми, які пройшли

вичерпні тести на наявність вразливих місць. Тому недостатня стійкість шифрограм за умови використання досконалих алгоритмів може зумовлюватися некваліфікованим застосуванням криптоалгоритмів чи бути наслідком використання «слабких» ключів. Засоби, розміщені в меню **Analysis**, дають можливість ознайомитися із основними методами криптоаналізу.

В підменю **Tools of Analysis** доступними є такі інструменти, що можуть використовуватися в криптоаналізі:

– **Entropy –** обчислює **ентропію** відповідного документа;

– **Floating Frequency – змінна частота** визначає, скільки різних символів знаходиться в кожних заданих 64-знакових сегментах документа;

– **Histogram – гістограма** у вигляді графіка ілюструє частість появи символів у документі;

– **N-Gram –** список до 5000 найчастіших **N-грам,** тобто наборів різних 1-, 2-, 3, … чи 16-ти символів у текстовому документі в порядку зменшення їх кількості;

– **Autocorrelation** – **автокореляція** документа надає кількісну оцінку подібності різних його частин і може використовуватися для визначення довжини ключа (див. рис.5);

– **Periodicity** – **циклічність** є параметром, який визначається як повторення певної послідовності **k≥1** символів від певної позиції до кінця документа.

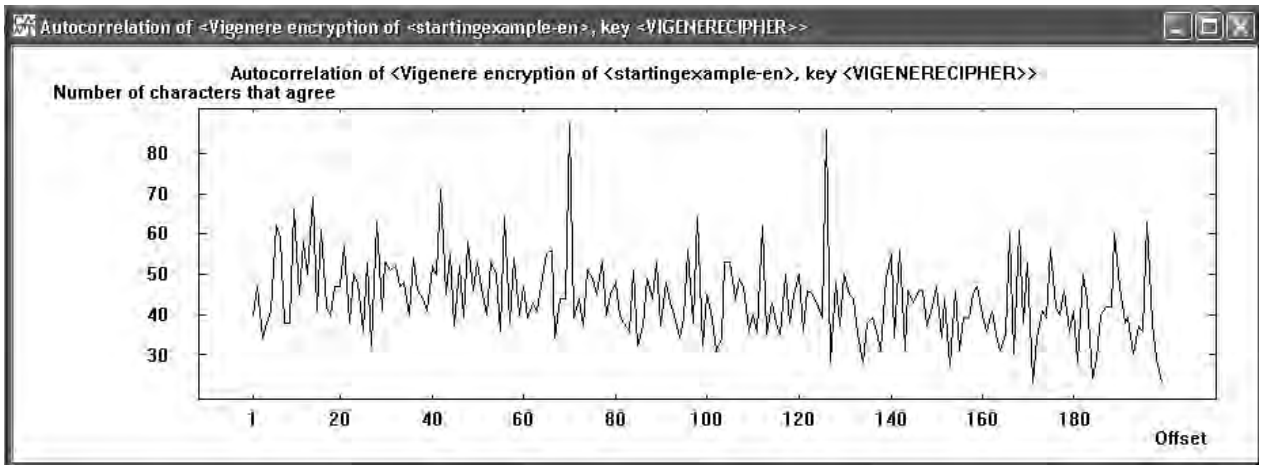

Рис. 5. Вигляд вікна автокореляції шифрограми

У підменю **Symmetric Encryption (classic)>Ciphertext-Only** для автоматичного криптоаналізу лише на основі шифрограми доступні такі класичні алгоритми, як **Caesar, Vignere, ADFGVX, Substitution, Solitaire, Addition** і **XOR,** а в підменю **Symmetric Encryption (classic)>Manual Analysis** можливий керований користувачем криптоаналіз шифрів **Substitution, Playfair** і **Solitaire.**

Підменю **Symmetric Encryption (modern)** містить засоби для автоматичного криптоаналізу шифрограм, одержаних із використанням всіх 15 симетричних блокових алгоритмів в меню **Crypt/Decrypt.** Криптоаналіз здійснюється шляхом повного перебору заданого користувачем простору ключів (**brute-force attack**). Після дешифрування за всіма можливими ключами за правильно відкритий текст приймають версію із найменшою ентропією перших тисячі знаків.

Підменю **Asymmetric Encryption** надає користувачу деякі засоби криптоаналізу алгоритму RSA, зокрема факторизацію числа на прості множники на основі таких відомих методів і алгоритмів, як **Brute-force, Brent, Pollard, Williams, Lenstra і Quadratic sieve.**

Підменю **Hash** дає змогу аналізувати різних хеш-алгоритми на предмет знаходження колізії за так званим парадоксом дня народження.

Підменю **Analyse Randomness** надає користувачу різні інструменти, щоб проаналізувати якість випадкових послідовностей за допомогою різноманітних тестів.

7. Висновок. Оцінка застосування пакета CrypTool у навчальному процесі

Використання пакета CrypTool у навчальному процесі на кафедрі захисту інформації Національного університету «Львівська політехніка» дає змогу зробити такі висновки. Наявні історичні шифри і засоби їх криптоаналізу мають не лише велике пізнавальне значення, але й дають можливість студентам ознайомитися зі змістом перетворень класичної криптографії. Проте текстові документи, які можна опрацьовувати у пакеті CrypTool, на жаль, не допускають використання кириличного алфавіту. Крім того, в наявному арсеналі інструментів криптоаналізу історичних шифрів не представлені методи Kasiski та Friedman (IC – індекс коінциденції).

У пакеті CrypTool набір симетричних блокових алгоритмів є повним, натомість із асиметричної криптографії всебічно можна досліджувати лише алгоритм RSA. Вбудовані засоби візуалізації і анімації стосовно сучасних симетричних і асиметричних криптоалгоритмів дають змогу відслідковувати зміст перетворень на кожному кроці, що полегшує розуміння студентами «внутрішньої» суті складних алгоритмів. Що стосується криптоаналізу сучасних блокових алгоритмів, реалізовано лише метод прямого перебору ключів. При цьому алгоритм відбору правильної версії серед множини дешифрованих документів ґрунтується лише на оцінці їх ентропії. Отже, криптоаналіз стає неможливим, якщо документ перед шифруванням був стиснений. Також слід зазначити, що режим CBC зв'язування блоків шифрограми алгоритму DES не передбачає використання початкового вектора ініціалізації, а відтак не дає змоги підняти стійкість шифрограм. Також не передбачена робота алгоритму DES у такому часто застосовуваному режимі, як зворотний зв'язок за шифрограмами (Ciphertext Feed Back – CFB).

Слід зазначити, що пакет CrypTool є лишень навчальною програмою і як криптологічний засіб не повинен застосовуватися у реальних системах захисту інформації. Пакет доступний в англійській, німецькій, іспанській та польській мовних версіях. До програми додається електронна версія підручника, що містить теоретичний вступ до сучасної криптології.

1. Buchmann J. Introduction to Cryptography, Springer, 2nd edition, 2004. – 335 p. 2. Шнайер Б. Прикладная криптография. – М.: Триумф, 2004. – 442 с. 3. Х.К.А. ван Тилборг. Основы Криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с. 4. Бабак В.П. Теоретичні основи захисту інформації: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с. 5. http://www.cryptool.com.