Використання CrypTool на прикладі симетричного шифру AES

Іван Савка, Юрій Яновський

Кафедра інформаційних технологій
ДВНЗ "Прикарпатський національний університет імені Василя Стефаника"
м.Івано-Франківськ, Україна

***Анотація*—Засоби візуалізації сучасних криптоалгоритмів у CryptoTool дають можливість відслідковувати зміст криптографічних перетворень на кожному кроці. Це дозволяє полегшити розуміння «внутрішньої» суті складних алгоритмів при розробці програмного забезпечення. Проводиться огляд можливостей використання CrypTool на прикладі шифру AES.**

Keywords—криптографічні алгоритми, CryptoTool, симетричний блочний шифр, шифр AES.

I. Вступ

CrypTool – це безкоштовне навчальне програмне забезпечення з відкритим кодом, що ілюструє криптографічні та криптоаналітичні концепції, дозволяє краще зрозуміти алгоритми шифрування і дешифрування, навчити користувачів протистояти мережевим загрозам, забезпечуючи безпеку своїх даних [1]. Проект започаткував професор Бернхард Есслінгер у 1998 році з метою підвищення кваліфікації співробітників банку в галузях IT-безпеки та криптографії та розвивався у декількох німецьких університетах (Дармштадт, Дуйсбург-Ессен, Зіген). CrypTool має п'ять версій CT1, CT2, JCT, CTO і MTC3, що використовуються в різних аспектах [1]. Зокрема, у статті [2] можна знайти детальний огляд та порівняльний аналіз версій, серед них виділено найбільш ефективні щодо реалізації алгоритмів шифрування та зручного інтерфейсу. Програма містить класичні та сучасні техніки шифрування, зокрема симетричні, асиметричні та гідридні криптографічні алгоритми, функції хешування, цифрові підписи тощо. Вона може демонструвати загрози та ризики, які можуть виникати при застосуванні криптографічних засобів захисту, застосовувати криптоаналіз та відомі атаки на криптографічні системи. Реалізований математичний апарат програми дозволяє визначити, чи є число простим, здійснювати генерацію простих чисел у заданому діапазоні, здійснювати розклад числа на прості множники (факторизацію числа), обчислення ентропії й автокореляції, підрахунок частоти появи символу або послідовності символів у тексті тощо. До програми CrypTool 2 (CT2) можна розробляти власні плагіни, які реалізують деякі криптографічні алгоритми або подібну функціональність [3].

II. Виклад основного матеріалу

До кожного вже реалізованого алгоритму у програмі дається коротке пояснення принципу його роботи, користувач може зашифрувати введений текст з відповідними параметрами алгоритму. Зашифрований текст буде відображатися після виконання поточної робочої області відповідного алгоритму. Розглянемо на прикладі шифру AES можливості інструментарію CrypTool 2. AES (Advanced Encryption Standard, відомий як Rijndael) є сучасним стандартом для симетричних блокових шифрів і активно використовується серед іншого в таких протоколах як SSL, SSH, Wireless LAN 802.11i тощо. При описі алгоритму використовується поле Галуа $GF(2^8)$, побудоване як розширення поля GF(2) за коренями деякого незвідного многочлена [4].

Щоб відкрити AES у версії CT2 можна скористатись відповідним шаблоном. Знайти його можна, наприклад, ввівши у фільтрі шаблонів рядок “AES”. Зокрема, шаблон AES Visualization відтворює покроковий процес шифрування 128-бітного повідомлення [5].

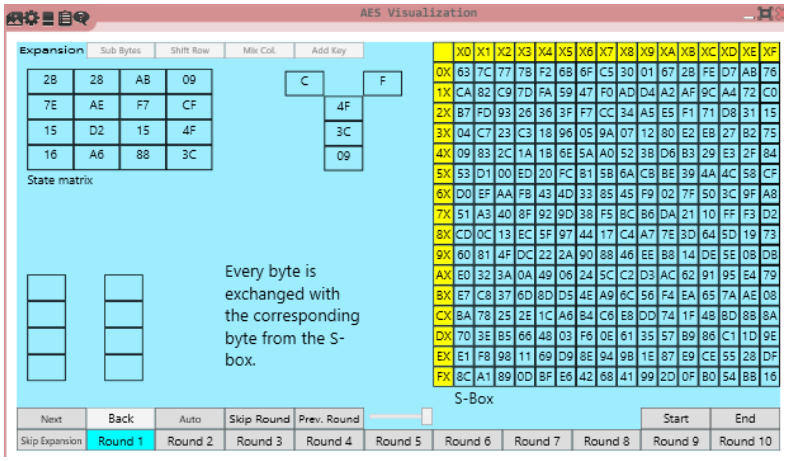

Рис. 1. *AES Visualization*

Інший шаблон AES Cipher (input text) можна використовувати для шифрування довільного тексту.

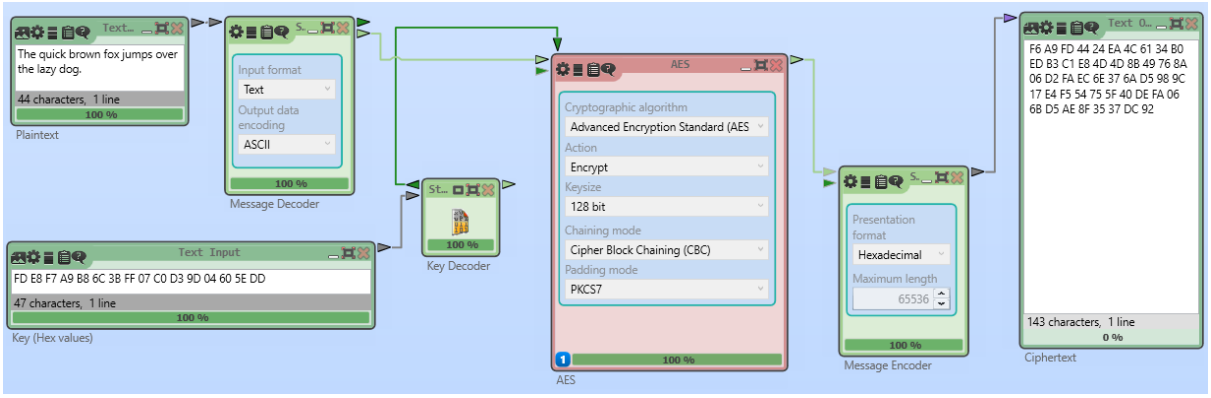

Рис. 2. *Шаблон AES Cipher (input text)*

Відкритий текст вводиться в компоненті Plaintext, а відповідний шифротекст отримується в компоненті Ciphertext після запуску шаблону. Оскільки компонент AES працює з байтами, то вихідний текст спочатку перетворюється в байти за допомогою компонента Message Decoder, в якому можна налаштувати формат та кодування відкритого тексту. Послідовність отриманого шифротексту перетворюється в шістнадцятковий формат з використанням компонента message encoder. Цей шаблон також можна використовувати для дешифрування повідомлень.

Компонент AES має кілька параметрів і використовує ключ. Такими параметрами є

- криптографічний алгоритм: це режим роботи AES/ Rijndael
- дія: зашифрувати або розшифрувати
- розмір ключа: кількість бітів у ключі 128/192/256
- режим ланцюга: як зашифровані дані з одного блоку використовуються в наступному
- режим заповнення: наприклад, заповнення блоків нулем менше розміру блоку AES

З іншого боку, CrypTool містить криптоаналіз алгоритму AES, зокрема AES – Ciphertext-only analysis.

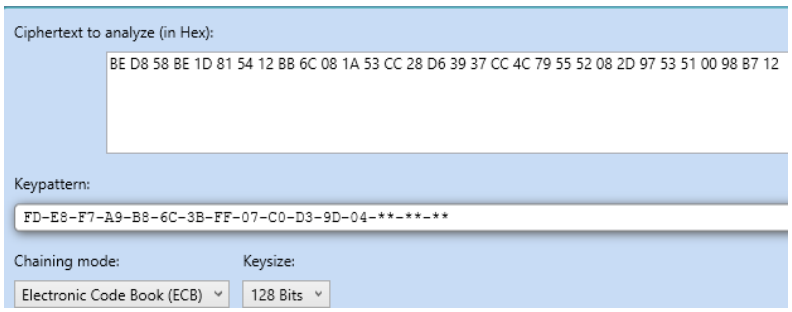

Рис. 3. *AES – Ciphertext-only analysis*

Наприклад, розшифрування криптотексту

C=«BE D8 58 BE 1D 81 54 12 BB 6C 08 1A 53 CC 28 D6 BF F6 25 1A E0 07 01 35 55 D9 99 48 E1 43 49 91»

за умови наявності часткової інформації про ключ

Keypattern = «FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 ** ** **»

де невідома частина позначена через *, здійснюється за 1 хв (Intel Core i5 2.7GHz 4GB RAM). Всього перебирається приблизно 16,8 млн. можливих ключів Атака використовує просту ентропію - зашифрований текст є більш хаотичним, ніж текст на мові.

Рис. 4. *Результат із найменшою ентропією – перший у стовпці "Value"*

III. Висновки

Cryptool – це зручний інструмент для використання в області криптографії, містить як готові шаблони, так і можливість побудови нових алгоритмів. Вбудовані засоби візуалізації та анімації математичних перетворень і сучасних криптоалгоритмів у CryptoTool дають доступне представлення і полегшують розуміння таких алгоритмів при захисті інформації та розробці відповідного програмного забезпечення.

Література

[1] The CrypTool Portal [Електронний ресурс]. – Режим доступу: http://www.cryptool.org/

[2] Загацька Н.О. Огляд різних версій пакету CrypTool як засобу захисту інформаційних ресурсів // Інформаційні технології і засоби навчання: електронне наукове фахове видання [Електронний ресурс] / Ін-т інформ. технологій і засобів навчання АПН України, Ун-т менеджменту освіти АПН України. – 2012. – № 5(31). – Режим доступу : http://journal.iitta.gov.ua/index.php/itlt/article/view/744/548.

[3] Przybylski, A. Wacker, M. Wander, F. Enkler, and P. Vacek: Plugin Developer Manual – How to build your own plugins for CrypTool 2, March 2016. https://www.cryptool.org/trac/CrypTool2/wiki

[4] Jun Ma, Jun Tao, Melissa Keranen, Jean Mayo, Ching-Kuang Shene, and Chaoli Wang: AESvisual: A Visualization Tool for AES Cipher, 2014. http://www.cs.mtu.edu/~shene/NSF-4/AESvisual.pdf

[5] Matthias Becher Visualization of AES as a CrypTool 2 Plugin. Bacherlor Thesis University of Mannheim, 2016. https://www.cryptool.org/images/ctp/documents/BA_Becher.pdf