Journal of educational equipment: Applied research, Volume 2, Issue 303 (December 2023)
ISSN 1859 - 0810

Quy trình ứng dụng công cụ Cryptool 2 trong giảng dạy và thực hành các thuật toán mật mã

Trần Đăng Ninh*

**Khoa Mật mã, trường Đại học Kỹ thuật – Hậu cần CAND*
Received: 5/11/2023; Accepted: 12/11/2023; Published: 29/11/2023

Abstract: *In this paper, we propose a procedure for applying CrypTool 2 in teaching and practicing cryptographic algorithms, from determining the operating scenarios of the algorithm, selecting modules and customizing them to fit usage requirements. The results show the potential application of the CrypTool 2 in educational and training activities cryptography, especially for novices who starts learning and researching cryptographic algorithms.*

Keywords: *CrypTool 2, cryptographic algorithms, cryptographic primitives, illustration, implementation*

1. Đặt vấn đề

Thuật toán mật mã là một trình tự, quy trình các quy tắc, bước thực hiện, hoặc phương trình toán học được xác định rõ ràng để mô tả quá trình biến đổi mật mã như mã hoá, giải mã, tạo khoá, xác thực, ký số… Việc giảng dạy và thực hành các thuật toán mật mã yêu cầu kiến thức cơ bản trong nhiều ngành khoa học khác nhau như toán học, xử lý tín hiệu, công nghệ thông tin, và viễn thông. Đây là một thách thức lớn không chỉ cho người giáo viên trong quá trình giảng dạy mà còn cho người học trong việc thực hành thuật toán mật mã. Tuy nhiên, những nghiên cứu về việc ứng dụng phần mềm trong giảng dạy và thực hành nội dung về các thuật toán mật mã ở các trường đại học cho đến nay còn ít được công bố. Tài liệu (W. Stalling 2020) cung cấp nhiều bài thực hành mật mã nhưng yêu cầu người đọc có trình độ về ngoại ngữ, kiến thức về mật mã và an toàn thông tin, tiêu tốn nhiều công sức chỉnh sửa cho phù hợp với mục tiêu, đối tượng, và nội dung đào tạo cụ thể. Các phần mềm ngoại tuyến như Crypt4Free, HashCalc, MD5… mang tính ứng dụng hơn là minh họa nguyên lý hoạt động, mang lại hiệu quả không cao trong hoạt động giảng dạy và thực hành. Trong khi đó, một số phần mềm trực tuyến yêu cầu kết nối mạng, chỉ cung cấp một số lượng cố định các thuật toán mật mã, hạn chế khả năng hiệu chỉnh cho phù hợp với nội dung giảng dạy. Vì vậy, người dạy và người học phải sử dụng các nguồn khác nhau trong cùng một môn học về mật mã.

Bộ công cụ CrypTool là một phần mềm giao diện đồ họa người dùng mã nguồn mở được thiết kế cho việc giảng dạy về mật mã học (The CrypTool Portal 1998-2023). Phần mềm CrypTool đã được sử dụng làm công cụ dạy học cho nhiều đối tượng người học khác nhau và được chứng minh là hiệu quả trong việc giảm sự phức tạp của việc giảng dạy các thuật toán mật mã (Yang, Wallace and Burchett 2011, Hick, Eslinger and Wacker 2012). Nghiên cứu của (Adamovic, et al. 2018) tiếp tục khẳng định tầm quan trọng của việc sử dụng các công cụ phần mềm như CrypTool trong học tập các thuật toán mật mã hiện đại. Tuy nhiên, những nghiên cứu này chỉ dừng lại ở việc thực thi hoặc minh họa một số thuật toán mật mã cụ thể, chưa có sự khái quát về cách ứng dụng trong giảng dạy và thực thành các thuật toán mật mã. Đối với người mới tìm hiểu về khoa học mật mã, việc sử dụng bộ công cụ CrypTool để thực hành các thuật toán mật mã sẽ gặp những khó khăn do thiếu phương pháp ứng dụng và quy trình thực hiện. Điều này thúc đẩy chúng tôi nghiên cứu ứng dụng công cụ CrypTool 2 trong giảng dạy và thực hành các thuật toán mật mã.

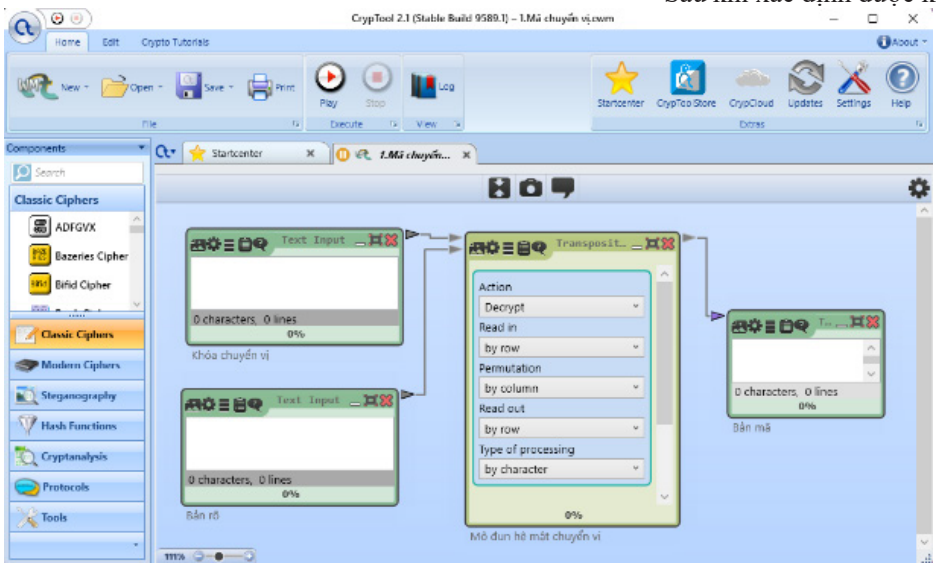
2. Nội dung nghiên cứu

2.1. Tổng quan về công cụ CrypTool 2

CrypTool 2 (CT2), cùng với 3 phần mềm khác là CrypTool-Online (CTO), CrypTool 1 (CT1), CrypTool 2 (CT2), và JcrypTool (JCT), thuộc bộ công cụ mã nguồn mở CrypTool. Mỗi công cụ đều cung cấp đa dạng các mô đun thuật toán mật mã và có những ưu điểm khác nhau. Trong khi CT1 và JCT cung cấp khả năng thực thi các thuật toán mật mã trong các ứng dụng thực tế và phù hợp với người đã có những hiểu biết cơ bản về khoa học mật mã, CTO và CT2 là những ứng dụng phù hợp cho việc giảng dạy và thực hành các nội dung về khoa học mật mã với người mới bắt đầu nghiên cứu lĩnh vực này. Đặc biệt, CT2 cung cấp phong phú số lượng các mô đun nguyên thủy mật mã giúp ích cho việc lựa chọn và thiết kế chương trình thực thi thuật toán mật mã. Đây

là một công cụ tốt và phù hợp cho việc giảng dạy và thực hành trong các cơ sở giáo dục đại học.

CT2 sử dụng một giao diện lập trình đồ họa, cung cấp khả năng thiết kế và thực thi thuật toán mật mã chỉ với thao tác kéo thả các mô đun đã được thiết kế sẵn, thể hiện như Hình 1. Người sử dụng sẽ chọn mô đun mật mã cần dùng, lựa chọn các mô đun nhập dữ liệu đầu vào và mô đun xuất dữ liệu đầu ra cho phù hợp với thuật toán mật mã lựa chọn. Tuỳ thuộc vào các thuật toán mật mã khác nhau, người dùng có thể phải thiết lập các tham số ban đầu trong mô đun mật mã trước khi chạy chương trình. Trong quá trình thực thi thuật toán mật mã, người sử dụng có thể thay đổi các giá trị đầu vào và quan sát được sự thay đổi của giá trị đầu ra.



Hình 2.1 Một chương trình thực thi thuật toán mật mã trong công cụ CrypTool 2

2.2. Quy trình ứng dụng CrypTool 2 thực thi các thuật toán mật mã

2.2.1. Xây dựng các kịch bản giảng dạy và thực hành

Các thuật toán mật mã có nguyên lý hoạt động rất đa dạng, từ đơn giản đến phức tạp. Trong quá trình giảng dạy và thực hành, phụ thuộc vào độ phức tạp của thuật toán mật mã mà người dạy/người học không chỉ tính toán dữ liệu đầu ra mà còn cần sự minh họa từng bước thực hiện của thuật toán. Bên cạnh đó, một số thuật toán có thể được thực hiện theo nhiều phương thức khác nhau tạo ra những kết quả đầu ra khác nhau với cùng các giá trị đầu vào. Vì vậy, trước khi sử dụng CT2 để thiết kế các chương trình thực thi, người dùng cần xác định kịch bản thực hành thuật toán mật mã.

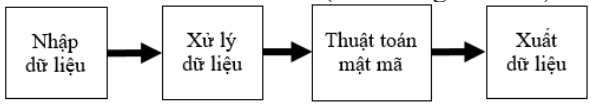
Một ví dụ xây dựng kịch bản với hệ mật AES có thể được mô tả như sau. Vì hệ mật AES có hoạt động phức tạp gồm nhiều bước và vòng lặp, việc giảng dạy hiệu quả cần có minh họa từng bước hoạt động của hệ mật này. Thêm vào đó, do mã khối có thể hoạt động với nhiều chế độ mã hoá/giải mã khác nhau, cần có chương trình thực thi trình hệ mật AES với cùng giá trị đầu vào và các chế độ hoạt động khác nhau.Như vậy, hai kịch bản cho hệ mật AES cần xây dựng gồm:

- Kịch bản thứ nhất, minh họa từng bước hoạt động cụ thể của AES.
- Kịch bản thứ hai, thực hiện hệ mật AES với cùng giá trị đầu vào và các chế độ hoạt động khác nhau.

2.2.2. Mô hình thiết kế chương trình thực thi

Sau khi xác định được kịch bản thực hành, người sử dụng sẽ lựa chọn mô đun mật mã thực hiện kịch bản đó và các mô đun nhập/xuất dữ liệu có định dạng phù hợp với các đầu vào/đầu ra. Mô hình thiết kế chương trình thực thi thuật toán mật mã được thể hiện như Hình 2.

Đối với khối nhập dữ liệu, CT2 cung cấp đa dạng các mô đun nhập dữ liệu như Audio Input (dữ liệu âm thanh), Camera (dữ liệu ảnh), File Input (dữ liệu tệp), Number Input (dữ liệu số), Text Input (dữ liệu ký tự), Boolean Input (dữ liệu nhị phân), Variable Load (dữ liệu dạng biến), Prime Generator (sinh số nguyên tố ngẫu nhiên), và Random Number Generator (sinh số ngẫu nhiên).



Hình 2.2 Mô hình thiết kế chương trình thực thi

Do mô đun thuật toán mật mã có thiết lập dạng dữ liệu đầu vào xác định, khối xử lý dữ liệu biến đổi dạng dữ liệu nhập vào thành dạng phù hợp mà mô đun thuật toán mật mã xử lý. Đối với khối xử lý dữ liệu, CT2 cung cấp đầy đủ các loại mô đun xử lý như Byte Array Operations (dữ liệu byte), Number Operation (dữ liệu số), String Operations (dữ liệu

chuỗi ký tự), Boolean Binary Operator (dữ liệu bit nhị phân), ImageProcessor (dữ liệu ảnh), CVSReader (dữ liệu bảng tính), Converter (chuyển đổi các dạng dữ liệu), String encoder/decoder (bộ mã hoá/giải mã mã ký tự), và Visual encoder/decoder (bộ mã hoá/giải mã mã vạch 2 chiều).

Đối với mô đun thuật toán mật mã, CT2 cung cấp hơn 150 mô đun thực thi các thuật toán mật mã cổ điển, mật mã hiện đại (gồm cả mật mã khoá đối xứng và khoá bất đối xứng), ẩn mã, hàm băm, thám mã, và giao thức mật mã. Ngoài việc sử dụng các mô đun có sẵn, người dùng hoàn toàn có thể sử dụng các mô đun xử lý dữ liệu để thực hiện các thuật toán mật mã. Ví dụ, CT2 không cung cấp mô đun sẵn thực hiện hệ mật ElGamal, việc thực hiện hệ mật này có thể được thực hiện sử dụng mô đun Number Operation với phép tính luỹ thừa theo modular và phép tìm phần tử nghịch đảo modular inverse.

Đối với khối xuất dữ liệu, CT2 cung cấp số lượng mô đun đầy đủ phục vụ yêu cầu biểu diễn dữ liệu ở đầu ra như Audio Output, Picture Output, File Output, Text Output, Boolean Output, Variable Store.

2.2.3. Khả năng tùy chỉnh mô đun mật mã

Trong giao diện lập trình của CT2, người sử dụng có thể điều chỉnh kích thước và một số cài đặt của các mô đun thiết kế sẵn. Tuy nhiên, những tuỳ chỉnh này được giới hạn ở những thay đổi được cho phép như cỡ chữ hiển thị, dạng dữ liệu xử lý, phương thức hiển thị, và một số cài đặt khác. Đối với những thay đổi lớn, mang tính thay đổi về bản chất như thêm số lượng đầu vào, đầu ra, điều chỉnh hoạt động của thuật toán mật mã, cần có sự can thiệp của phần mềm lập trình ngôn ngữ C# như Visual Studio. Mã nguồn của chương trình được công khai để người sử dụng có thể tuỳ chỉnh các mô đun mật mã và lập trình những mô đun mới. Một số video hướng dẫn về việc phát triển mô đun CT2 cá nhân được đăng tải trên kênh Youtube chính thức của dự án CT2 (N. Kopal n.d.).

2.3. Các kết quả đạt được

Căn cứ trên một số môn học về khoa học mật mã (Lý thuyết mật mã (ET3310) 2017), (Mật mã học cơ sở (INT1344) 2019), chúng tôi đã xây dựng 26 kịch bản thực hành cho 12 thuật toán mật mã, bao gồm mã dịch vòng, mã chuyển vị, mã Vigenere, tiêu chuẩn mã hóa dữ liệu DES, tiêu chuẩn mã hóa tiên tiến AES, mã dòng sử dụng thanh ghi dịch tuyến tính, mã dòng RC4, hệ mật RSA, hệ mật ElGamal, hàm băm MD5 và mã xác thực thông báo dựa trên hàm băm HMAC, giao thức trao đổi khóa Diffie – Hellman. Từ những kịch bản xây dựng được và căn cứ vào những mô đun được CT2 cung cấp, chúng tôi đã thiết kế được 42 chương trình thực thi theo 26 kịch bản thuật toán mật mã. Thư mục công khai chia sẻ các kịch bản thực hành và chương trình thực thi thuật toán mật mã này sử dụng công cụ CT2 có địa chỉ tại https://github.com/DNT-T07/CrypTool-2.

3. Kết luận

Bài báo đề đưa ra được một quy trình trong ứng dụng công cụ CrypTool 2 trong giảng dạy và thực hành thuật toán mật mã trong các chương trình đào tạo khoa học mật mã. Người sử dụng cần xây dựng kịch bản cho việc giảng dạy hoặc thực hành thuật toán mật mã trước khi lựa chọn các mô đun thiết kế sẵn được CT2 cung cấp và tuỳ chỉnh các mô đun cho phù hợp với yêu cầu. Các kết quả cho thấy tính khả thi và sự linh hoạt khi ứng dụng công cụ này trong hoạt động giảng dạy và thực hành với các đối tượng và nội dung đào tạo khác nhau. Hướng nghiên cứu tiếp theo có thể là việc ứng dụng bộ công cụ CrypTool này trong hình thức học tập trực tuyến hoặc kết hợp trực tuyến – trực tiếp.

Tài liệu tham khảo

Adamovic, S., M. Sarac, D. Stamenkovic, and D. Radovanovic. 2018. “The importance of the Using Software Tools for Learning Modern Cryptography.” *Int. J. of Engineering Education.*

Hick, S., B. Eslinger, and A. Wacker. 2012. “Reducing the Complexity of Understanding Cryptology using CrypTool,.” *Int. Conf. on Education and Information Systems, Technologies and Applications.* Orlando, Florida, USA.

2017. “Lý thuyết mật mã (ET3310).” *Chương trình chuẩn Kỹ thuật Điện tử Viễn thông, Trường Điện - Điện tử, Đại học Bách Khoa Hà Nội.*

2019. “Mật mã học cơ sở (INT1344).” *Chương trình đào tạo ngành An toàn thông tin, Học viện Bưu chính viễn thông.*

N. Kopal. n.d. *Cryptography for everybody.* Accessed December 1st, 2023. https://www.youtube.com/@CryptographyForEverybody.

1998-2023. *The CrypTool Portal.* https://www.cryptool.org.

W. Stalling. 2020. *Cryptography and Network Security: Principles and Practice.* Harlow, Essex, England: Pearson.

Yang, R., L. Wallace, and I. Burchett. 2011. “Teching Cryptology At All Levels Using CrypTool.” *Colloquium for Information Systems Security Education.* Fairborn, Ohio, USA.