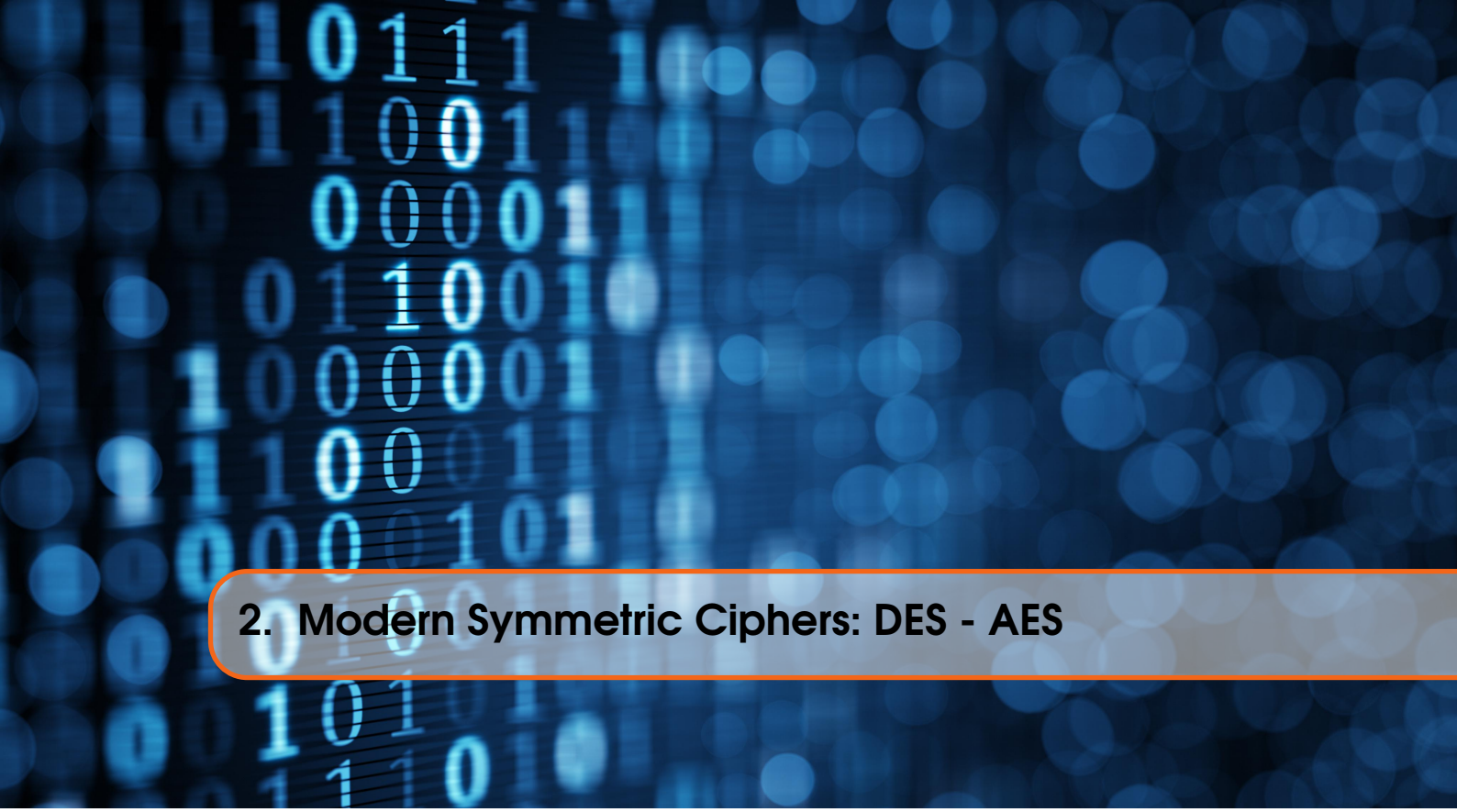


2. Modern Symmetric Ciphers: DES - AES

2.1 TỔNG QUAN

Trong các phương pháp mã hóa cổ điển, đối tượng mã hóa chính là các bản tin ngôn ngữ, đơn vị mã hóa là các chữ cái để áp dụng phương thức thay thế hay phương thức hoán vị. Với sự phát triển nhanh chóng và đa dạng của thông tin với nhiều định dạng khác nhau, việc biểu diễn trên máy tính được thể hiện qua các bit nhị phân.
Ví dụ:
Bản tin: **attack**
Mã ASCII: **97 116 116 97 99 107**
Biểu diễn nhị phân: **01100001 01110100 01110100 01100001 01100011 01101011**
Tương tự như bản tin ngôn ngữ, trong bản tin nhị phân cũng tồn tại một số đặc tính thống kê nào đó mà người phá mã có thể tận dụng để phá bản mã, dù rằng bản mã bây giờ tồn tại dưới dạng nhị phân. ***Mã hóa hiện đại*** quan tâm đến vấn đề chống phá mã trong các trường hợp biết trước bản rõ *(known-plaintext)*, hay bản rõ được lựa chọn *(chosen-plaintext)*.
Bài thực hành này sẽ tập trung vào thuật toán mã hóa đối xứng hiện đại, tập trung chính vào chuẩn mã hóa dữ liệu **DES** *(Data Encryption Standards)* để minh họa cho kiểu mã hóa khối.

2.1.1 Kiến thức nền tảng

Để thực hành tốt, sinh viên cần nắm được kiến thức về:
- Mã hóa khối (Block Cipher) cơ bản.
- Mô hình mã SP, mã khối Feistel.
- Quy trình mã hóa, các vòng và thuật toán của DES (Data Encryption Standards).
- Các mô hình ứng dụng mã khối như ECB, CBC, CTR,...

Những nội dung trên, sinh viên có thể tham khảo tại:
[1] Chapter 3: Block Cipher and the Data Encryption Standards - W. Stallings, *Cryptography and network security: Principles and practice, 6th ed*. Boston, MA, United States: Prentice Hall, 2013

2.1.2 Môi trường - Công cụ

1. Máy tính Windows và IDE với ngôn ngữ lập trình tùy ý (C#, Java, Web,...)
2. Phần mềm **CrypTool 1.4.31** hoặc **CrypTool 2.1**
   CrypTool được cung cấp miễn phí tại `https://www.cryptool.org` (sử dụng phiên bản 1.4.31 hoặc 2.1). CrypTool 2.1 là phiên bản mới của CrypTool truyền thống với khả năng hỗ trợ mạnh mẽ hơn trong việc mã hóa/ giải mã và đặc biệt là mô phỏng hoạt động của các thuật toán mã hóa.

2.2 NỘI DUNG THỰC HÀNH

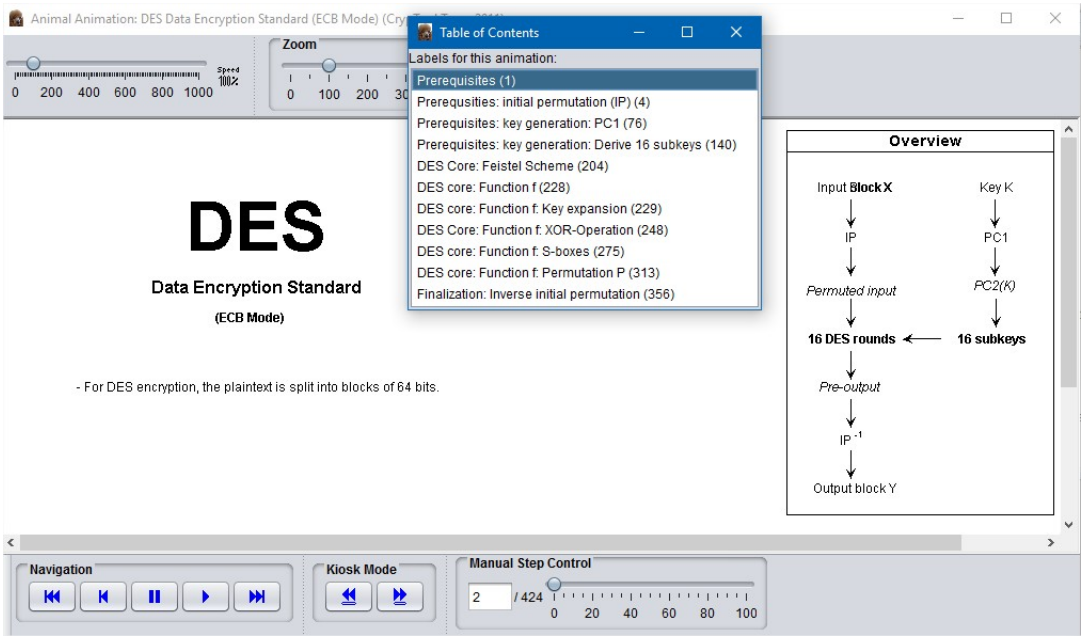
Lab 2 gồm 1 buổi thực hành với thời lượng 5 tiết/buổi theo kế hoạch 6 buổi thực hành.

2.2.1 Mã hóa DES

Task 2.1 CrypTool 1 và CrypTool 2 đều hỗ trợ mô phỏng *(Visualization)* mã hóa DES chi tiết và cụ thể qua từng bước.
Sinh viên tự chọn sử dụng *CrypTool 1* hoặc *CrypTool 2* để mô phỏng thuật toán DES và dựa vào đó trình bày cách hoạt động của mã hóa DES qua các giai đoạn. ■

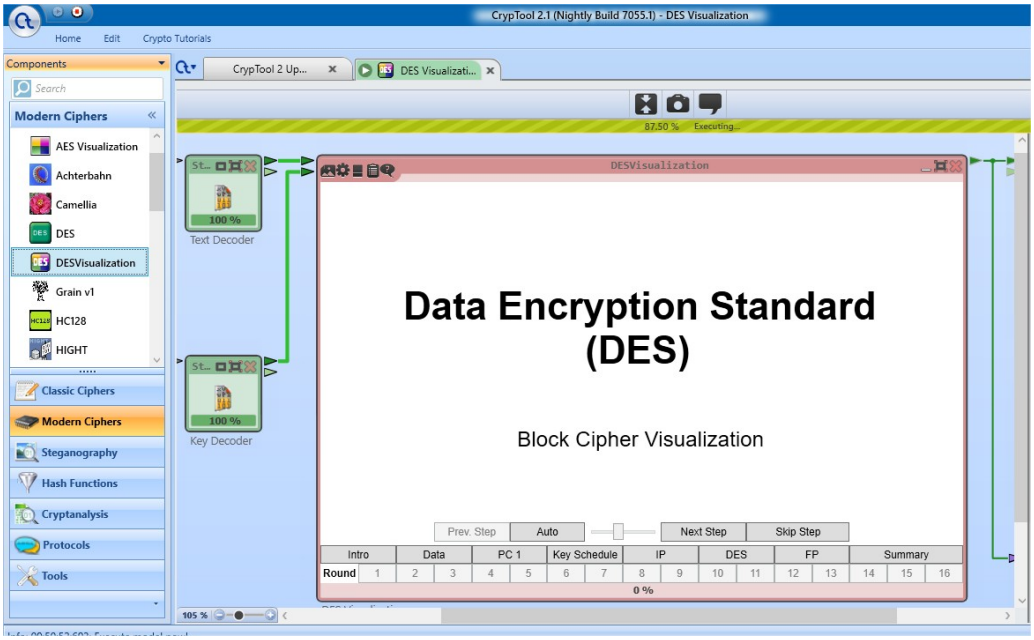
Gợi ý 2.1. *Mô phỏng DES trên CrypTool 1 và 2:*

1. *Trên **CrypTool 1**, để thực hiện mô phỏng DES, ta vào Indiv. Procedures » Visualization of Algorithms » DES. Sau đó, điều khiển việc mô phỏng tại phần Navigation để theo dõi cách hoạt động của DES dựa vào Input và key có sẵn.*
   Cửa sổ Tables of Contents thể hiện các giai đoạn chính của DES.



Hình 2.1: Mô phỏng thuật toán mã hóa DES trên CrypTool 1

2. *Trên **CrypTool 2**, để thực hiện mô phỏng DES, ta vào Startcenter » Templates » Cryptography » Modern » Symmetric » DES Visualization hoặc tự xây dựng mô hình theo các khối bằng cách chọn New và kéo thả các khối tương ứng.*
   Các giai đoạn chính của DES sẽ được thể hiện trực tiếp.



Hình 2.2: Mô phỏng thuật toán mã hóa DES trên CrypTool 2

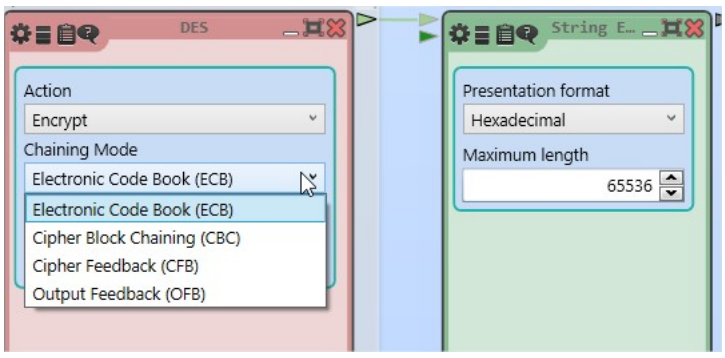
Task 2.2 Sử dụng CrypTool 2 để tiến hành mã hóa với nội dung sau:
- Plaintext: **UNIVERSITY OF INFORMATION TECHNOLOGY**
- Key: **0F 15 71 C9 47 D9 E8 59**

Lần lượt mã hóa Plaintext trên bằng các thuật toán mã hóa sau để tìm Ciphertext tương ứng dưới dạng Hex:

a. DES (mode ECB)
b. DES (mode CBC)
c. DES (mode CFB)
d. DES (mode OFB)

Tìm hiểu và so sánh sự khác nhau giữa 4 Channing Mode ECB, CBC, CFB và OFB ■

Gợi ý 2.2. *CrypTool 1 chỉ hổ trợ 2 mode ECB và CBC. Khi sử dụng CrypTool 2, để thiết lập nhanh mô hình DES Cipher, ta vào Startcenter » Templates để chọn DES Cipher. Trong khối mã hóa DES, có thể thiết lập các Channing Mode khác nhau và cũng có thể thay đổi định dạng Output thành Hexadecimal.*



Hình 2.3: Các Channing Mode hỗ trợ tại CrypTool 2

2.2.2 Tính lan truyền (Avalanche Effect)

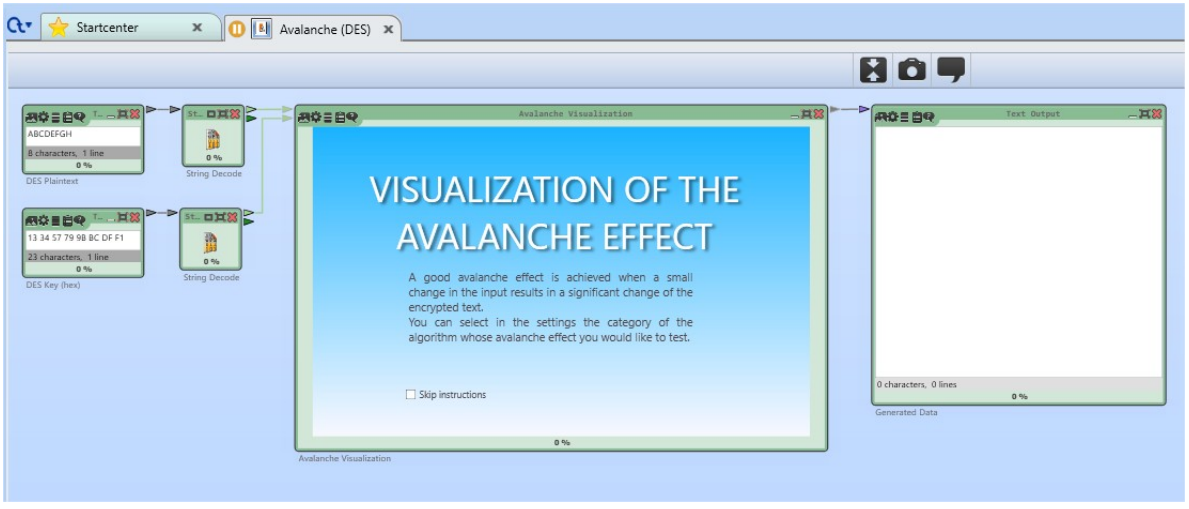
Một tính chất quan trọng cần thiết của mọi thuật toán mã hóa là chỉ cần một thay đổi nhỏ trong bản rõ hay trong khóa sẽ dẫn đến thay đổi lớn trong bản mã.
Ví dụ chỉ cần thay đổi 1 bit trong plaintext hay key thì sẽ ảnh hưởng đến thay đổi nhiều bit trong ciphertext - đây là tính chất lan truyền và mã hóa DES cũng có tính chất này.

Task 2.3 Cho cặp plaintext và key sau:
+ Plaintext: **KHOAMMTT**
+ Key(hex): **AE BC 12 34 56 78 32 56**

1. Xác định ciphertext tương ứng khi sử dụng mã hóa DES.
2. Giữ nguyên key, thay đổi các bit trong plaintext sao cho plaintext thành **KHOAMMTV**. Kiểm tra, so sánh số bit khác nhau và mức độ ảnh hưởng do lan truyền (%) của ciphertext sau từng vòng khi dùng mã hóa DES với thay đổi trên.
3. Giữ nguyên plaintext, thay đổi 1 bit bất kỳ trong key và kiểm tra so sánh số bit khác nhau và mức độ ảnh hưởng do lan truyền (%) qua từng vòng khi dùng mã hóa DES nếu thực hiện thay đổi trên.
4. Áp dụng đồng thời 2 thay đổi trên và thực hiện yêu cầu tương tự. Nhận xét về mức độ ảnh hưởng khi thực hiện các thay đổi trên trong mã hóa DES.

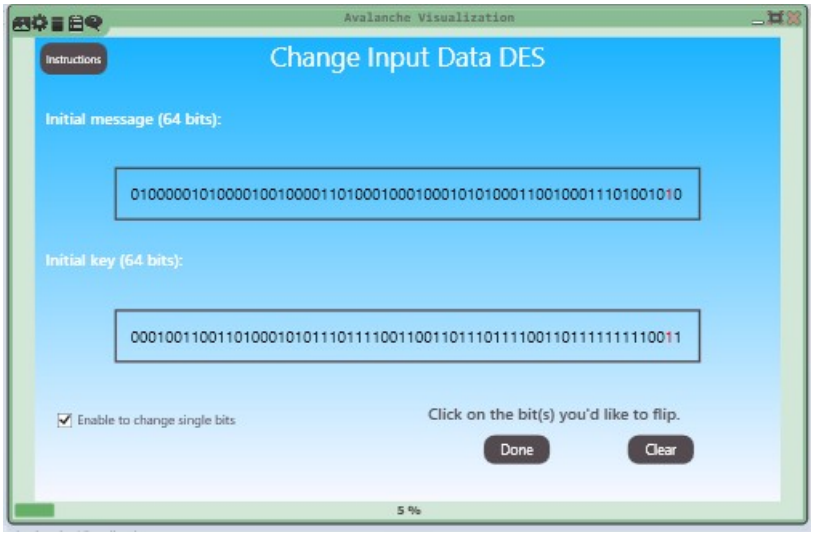
■

Gợi ý 2.3. *Trong CrypTool 2 có hỗ trợ mô phỏng hiệu ứng lan truyền và xác định mức độ ảnh hưởng khi thay đổi các bit nhất định trong mã hóa DES/AES. Sinh viên có thể sử dụng chức năng này tại* ***Startcenter » Templates » Modern » Avalanche (DES).***



Hình 2.4: Mô phỏng hiệu ứng lan truyền của DES trong CrypTool 2

Sinh viên cung cấp DES Plaintext, DES Key và bắt đầu quá trình mô phỏng. Chọn ***Enable to change single bits****, thực hiện các thay đổi và chọn* ***Done*** *để kiểm tra kết quả qua 16 vòng của DES.*



Hình 2.5: Thay đổi bit trong khối Avalanche Visualization

2.2.3 Độ an toàn của DES

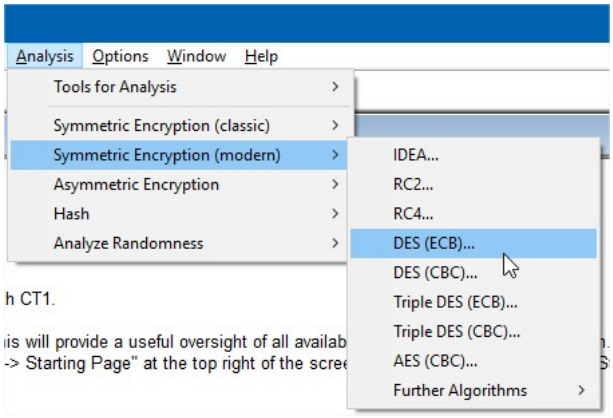
Task 2.4 Kiểm tra bằng cách tấn công vét cạn khóa *(brute-force attack)* với ciphertext sau đã được mã hóa theo mode ECB bằng CrypTool 1 và 2:

95 C8 EA FE 7B E9 5D BD 70 65 DE 31 62 8C 90 8A E4 16 98 18 E1 DC DE 83 00 A1 22 5D EF 6E AA C6 F1 80 12 08 CB DA 0D 22

Xác định thời gian cần thiết để brute-force và key, plaintext (nếu có thể) với từng trường hợp.

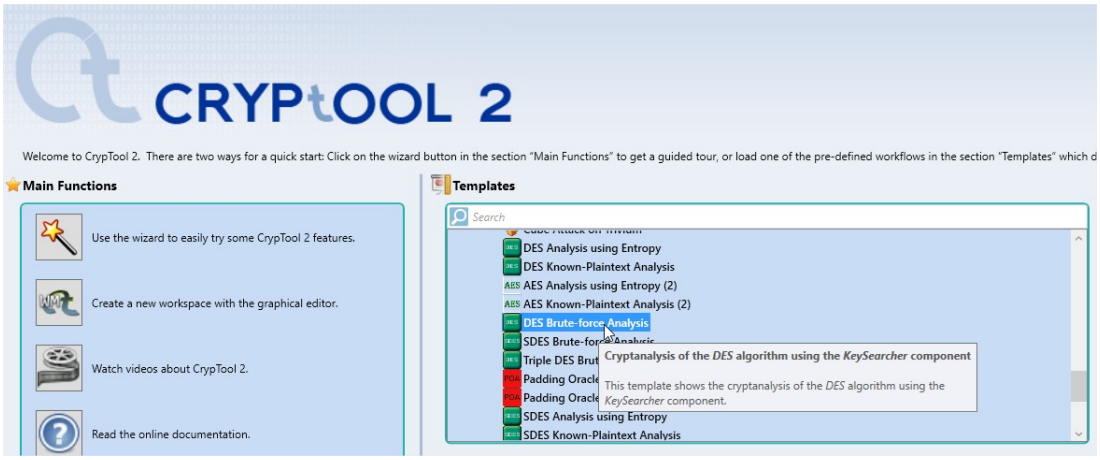
1. Chưa xác định được key (8 bytes)
2. Biết key bắt đầu với dạng 11-11-**-**-**-**-**-**
3. Biết key bắt đầu với dạng 11-11-11-11-**-**-**-**

Gợi ý 2.4. *Trong CrypTool 1 và 2 đều có hỗ trợ vét cạn khóa DES.*
*- Với CrypTool 1: Vào menu **Analysis » Symmetric Encryption (modern) » DES (ECB)***



Hình 2.6: Brute-force DES trong CrypTool 1

*- Với CrypTool 2: Vào **Startcenter » Templates » Cryptanalysics » Modern » DES Brute-force Analysics** (thay khối đầu vào của Key Searcher bằng Text Input và cung cấp Ciphertext trên)*

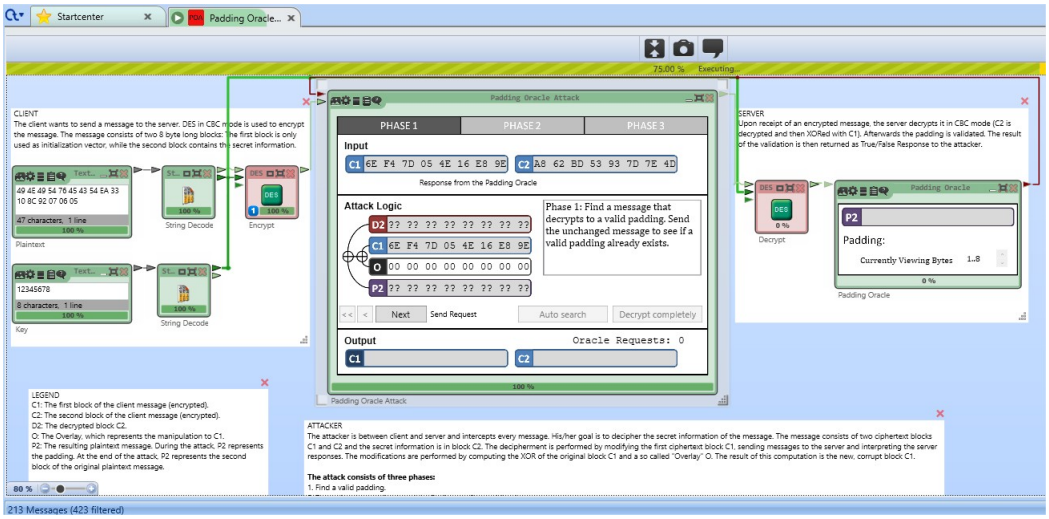


Hình 2.7: Brute-force DES trong CrypTool 2

2.2.4 Mở rộng

Mở rộng 2.1 Tấn công Padding Ocracle Attack trên DES

Padding Ocracle Attack (POA) là phương thức tấn công mạnh mẽ giúp giải mã ciphertext mã hóa với DES theo mode CBC mà không cần quan tâm đến key. POA dựa vào các padding (bit được thêm vào để làm đầy block cuối cùng), từ đó giải ngược để tìm toàn bộ phần còn lại của ciphertext. CrypTool 2 có mô phỏng kiểu tấn công này, sinh viên tham khảo và thử nghiệm, mô tả lại quá trình thực hiện Padding Ocracle Attack trên DES.



Hình 2.8: Padding Ocracle Attack trên DES trong CrypTool 2

Mở rộng 2.2 Sinh viên trình bày lại các bước hoạt động chính của mã hóa **AES** dựa vào chức năng mô phỏng trên CrypTool 1 hoặc 2 (Tương tự Task 2.1).

Mở rộng 2.3 So sánh các loại mã hóa DES, Triple-DES (3DES) và AES. Tại 2-DES không được sử dụng mà chỉ có DES, 3-DES?

2.3 YÊU CẦU - ĐÁNH GIÁ

2.3.1 Yêu cầu

Sinh viên thực hiện đầy đủ các nội dung trong phần thực hành theo nhóm (tối đa **2** sinh viên/nhóm) hoặc cá nhân *(đăng ký từ buổi 1)* và báo cáo kết quả thực hiện như sau:

- File báo cáo .pdf kết quả thực hiện các nội dung thực hành (theo mẫu).
- Đối với các ứng dụng, đặt vào thư mục có tên tương ứng với Task *(source code và file thực thi)*

Báo cáo trình bày trực quan việc thực hành có kèm hình ảnh và chú thích rõ ràng theo cách tiếp cận của bản thân, không sao chép lẫn nhau. Nếu có tham khảo cần ghi nguồn.

R Thời gian hoàn thành Lab 2:
Trong tối đa **10** ngày từ buổi thực hành tại lớp.

Lưu ý 2.3.1 Đặt tất cả báo cáo và thư mục liên quan vào 1 tập tin nén (.zip,.rar) có tên:

[MSSV1]-[Tên SV1]_[MSSV2]-[Tên SV2]_MMH_LabX

Ví dụ: 16520901-Nhut_16521516-Lam_MMH_Lab2. Kích thước tối đa: 10MB.
Nộp báo cáo theo thời gian quy định tại website môn học.

2.3.2 Đánh giá

- Sinh viên hiểu và hoàn thành tốt nội dung thực hành, đúng hạn: 80%
- Sinh viên trình bày cụ thể, rõ ràng kết quả thực hiện: 5-10%
- Khuyến khích sinh viên có tìm hiểu, thực hiện các nội dung mở rộng: 15-20% hoặc cộng trực tiếp vào điểm tổng kết thực hành nếu hoàn thành xuất sắc. *Nội dung mở rộng khuyến nghị thực hiện với sinh viên lớp ANTN.*
- Sao chép bài của sinh viên khác, tham khảo không ghi nguồn: -50% đến -100%.
- Nộp bài trễ: -20% mỗi ngày nộp trễ.

Lưu ý 2.3.2 Báo cáo nộp trễ, sao chép sẽ được xử lý tùy theo mức độ. Các nội dung báo cáo có thể được vấn đáp để đánh giá kết quả tại buổi thực hành tiếp theo, sinh viên vắng thực hành không có lý do thì nhóm sinh viên tương ứng sẽ được trừ tối thiểu 30% điểm bài thực hành đó.

2.4 TÀI LIỆU THAM KHẢO

[1] W. Stallings, *Cryptography and network security: Principles and practice, 6th ed*. Boston, MA, United States: Prentice Hall, 2013. *Chapter 3. Block Ciphers and the Data Encryption Standard*
[2] Bernhard Esslinger, *Learning and Experiencing Cryptography with CrypTool and SageMath, 12th ed*, CrypTool Project. Available: `https://www.cryptool.org/en/ctp-documentation`.

TÀI LIỆU THỰC HÀNH MẠNG MÁY TÍNH - AN TOÀN THÔNG TIN - UIT
Biên soạn - Tổng hợp: KS. Nguyễn Thanh Hòa

Tài liệu được tổng hợp, tham khảo và biên soạn phục vụ cho việc hướng dẫn thực hành các môn học tại bộ môn An toàn thông tin - Khoa Mạng máy tính và truyền thông.
Tài liệu thực hành này chỉ được sử dụng và cung cấp nội bộ tại website môn học trường ĐH Công nghệ Thông tin `https://courses.uit.edu.vn` cho các sinh viên tham gia các khóa học tương ứng. Tài liệu thực hành này chỉ sử dụng và **lưu hành nội bộ**, phục vụ cho việc học tập, nghiên cứu, không sử dụng và chia sẻ với các mục đích khác khi chưa có sự cho phép của Giảng viên.
Email liên hệ GV khi cần thiết: *hoant@uit.edu.vn*

Biên soạn Tháng 1/2017
Cập nhật lần 1 - Tháng 2/2018

LƯU HÀNH NỘI BỘ