Week 4 Practical: *Data Encryption System (DES)*

Dr. Qublai K. Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

Overview

1. Recap
2. DES Visualisation
3. DES in CryptTool 2
4. SDES
5. 3DES
6. Bringing it all together
7. Post-sessional work

UNIVERSITY OF GLOUCESTERSHIRE

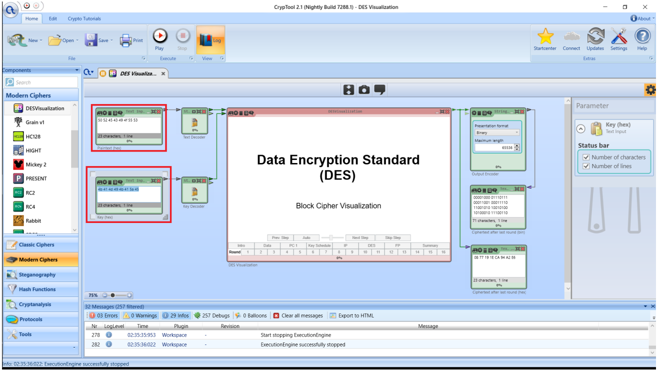
Recap

- Last week we looked at *ADFGVX cipher* and *Vernam cipher*
- We also looked at how each of them works and how they can be implemented in CryptTool 2
- This week we will be looking at *Data Encryption System*

DES Visualisation

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *DES Visualisation*
- In the Plaintext box, type in: `50 52 45 43 49 4f 55 53` (hex for PRECIOUS)
- In the Key box, type in: `4b 41 4d 49 4b 41 5a 45` (hex for: *KAMIKAZE*)
- Finally click on the *Play* button to execute

DES Visualisation



CrypTool 2.1 (Nightly Build 7288.1) - DES Visualization

Plaintext (hex): 50 52 45 43 49 4f 55 53 — 23 characters, 1 line

Key (hex): 4b 41 4d 49 4b 41 5a 45 — 23 characters, 1 line

Output Encoder: Presentation format: Binary; Maximum length: 65536

Ciphertext after last round (bin):

```
00001000 01110111
00011001 00011110
11001010 10010100
10100010 11100110
```

71 characters, 1 line

Ciphertext after last round (hex): 08 77 19 1E CA 94 A2 E6 — 23 characters, 1 line

Data Encryption Standard (DES)

Block Cipher Visualization

32 Messages (257 filtered)

03 Errors | 0 Warnings | 29 Infos | 257 Debugs | 0 Balloons | Clear all messages | Export to HTML

Nr	LogLevel	Time	Plugin	Revision	Message
278	●	02:35:35:953	Workspace	-	Start stopping ExecutionEngine
282	●	02:35:36:022	Workspace	-	ExecutionEngine successfully stopped

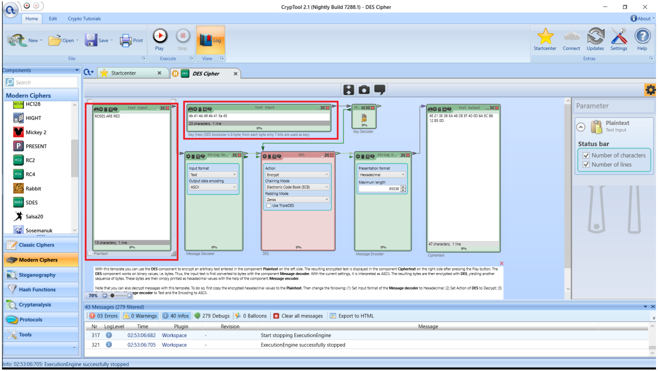
Info: 02:35:36:022: ExecutionEngine successfully stopped

Figure: DES Visualisation

DES in CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *DES Cipher*
- In the Plaintext box, type in: `ROSES ARE RED`
- In the Key box, type in: `4b 41 4d 49 4b 41 5a 45` (hex for: *KAMIKAZE*)
- Finally click on the *Play* button to execute

DES in CryptTool 2



Plaintext (Text Input): ROSES ARE RED — 13 characters, 1 line — 0%

Key (Text Input): 4b 41 4d 49 4b 41 5a 45 — 23 characters, 1 line — 0%

Key (hex) (DES blocksize is 8 byte; from each byte only 7 bits are used as key)

Message Decoder: Input format: Text; Output data encoding: ASCII — 0%

DES: Action: Encrypt; Chaining Mode: Electronic Code Book (ECB); Padding Mode: Zeros; ☐ Use TripleDES — 0%

Message Encoder: Presentation format: Hexadecimal; Maximum length: 65536 — 0%

Ciphertext (Text Output): 6E 21 3E 3B EA 48 DE EF 40 0D 8A EC B8 12 B5 0D — 47 characters, 1 line — 0%

Parameter: ☑ Number of characters ☑ Number of lines

With this template you can use the **DES** component to encrypt an arbitrary text entered in the component **Plaintext** on the left side. The resulting encrypted text is displayed in the component **Ciphertext** on the right side after pressing the Play button. The **DES** component works on binary values, i.e. bytes. Thus, the input text is first converted to bytes with the component **Message decoder**. With the current settings, it is interpreted as ASCII. The resulting bytes are then encrypted with **DES**, yielding another sequence of bytes. These bytes are then simply printed as hexadecimal values with the help of the component **Message encoder**.

Note that you can also decrypt messages with this template. To do so, first copy the encrypted hexadecimal values to the **Plaintext**. Then change the following: (1) Set Input format of the **Message decoder** to Hexadecimal; (2) Set Action of **DES** to Decrypt; (3) [illegible] **age encoder** to Text and the Encoding to ASCII.

```
43 Messages (279 filtered)
03 Errors | 0 Warnings | 40 Infos | 279 Debugs | 0 Balloons | Clear all messages | Export to HTML

Nr   LogLevel  Time          Plugin     Revision  Message
317  i         02:53:06:682  Workspace  -         Start stopping ExecutionEngine
321  i         02:53:06:705  Workspace  -         ExecutionEngine successfully stopped

Info: 02:53:06:705: ExecutionEngine successfully stopped
```

Figure: DES in CryptTool 2

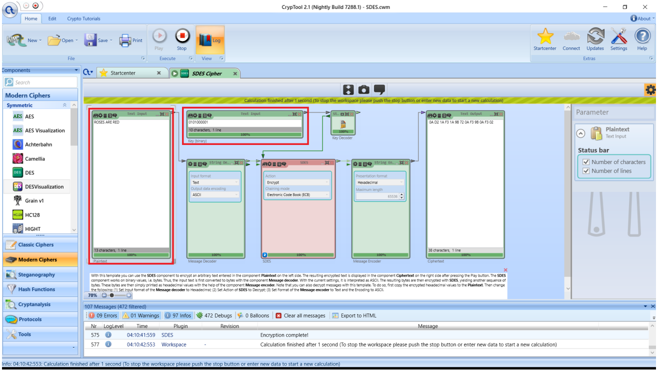
Simplified DES (SDES)

- Uses the same steps/components as regular DES
- Key differences lie in terms of:
  - Block size: Blocks of 12 bits instead of 64 bits
  - Key size: Only 9 bits instead of 56 bits
- Intended to be used for *experimental* purposes

SDES on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *SDES*
- In the Plaintext box, type in: `ROSES ARE RED`
- In the Key box, type in: 0101000001
- Finally click on the *Play* button to execute

SDES in CryptTool 2



Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)

Plaintext: ROSES ARE RED — 13 characters, 1 line

Key (binary): 0101000001 — 10 characters, 1 line

Message Decoder: Input format: Text; Output data encoding: ASCII

SDES: Action: Encrypt; Chaining mode: Electronic Code Book (ECB)

Message Encoder: Presentation format: Hexadecimal; Maximum length: 65536

Ciphertext: 0A D2 1A F3 1A 9B 72 0A F3 9B 0A F3 02 — 38 characters, 1 line

☑ Number of characters
☑ Number of lines

With this template you can use the **SDES** component to encrypt an arbitrary text entered in the component **Plaintext** on the left side. The resulting encrypted text is displayed in the component **Ciphertext** on the right side after pressing the Play button. The **SDES** component works on binary values, i.e. bytes. Thus, the input text is first converted to bytes with the component **Message decoder**. With the current settings, it is interpreted as ASCII. The resulting bytes are then encrypted with **SDES**, yielding another sequence of bytes. These bytes are then simply printed as hexadecimal values with the help of the component **Message encoder**. Note that you can also decrypt messages with this template. To do so, first copy the encrypted hexadecimal values to the **Plaintext**. Then change the following: (1) Set Input format of the **Message decoder** to Hexadecimal; (2) Set Action of **SDES** to Decrypt; (3) Set Format of the **Message encoder** to Text and the Encoding to ASCII.

107 Messages (472 filtered)

09 Errors | 01 Warnings | 97 Infos | 472 Debugs | 0 Balloons | Clear all messages | Export to HTML

```
Nr   LogLevel  Time          Plugin     Revision  Message
575            04:10:41:559  SDES                 Encryption complete!
577            04:10:42:553  Workspace  -         Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)
```

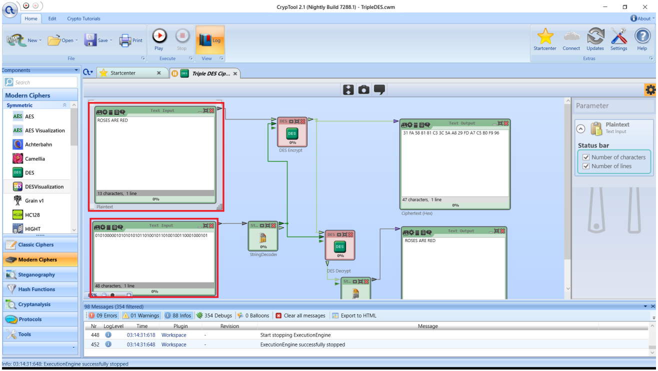
Info: 04:10:42:553: Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)

Figure: SDES in CryptTool 2

3DES on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *Triple DES*
- In the Plaintext box, type in: `ROSES ARE RED`
- In the Key box, type in: 010100000101010101011010010110100100110001000101 (binary for: *PUZZLE*)
- Finally click on the *Play* button to execute

3DES on CryptTool 2



CrypTool 2.1 (Nightly Build 7288.1) - TripleDES.cwm

Text Input (Plaintext): ROSES ARE RED
13 characters, 1 line

Text Input: 010100000101010101011010010110100100110001000101
48 characters, 1 line

Text Output (Ciphertext (Hex)): 31 FA 58 81 81 C3 3C 5A A8 29 FD A7 C5 B0 F9 96
47 characters, 1 line

Text Output: ROSES ARE RED

98 Messages (354 filtered)

09 Errors | 01 Warnings | 88 Infos | 354 Debugs | 0 Balloons | Clear all messages | Export to HTML

```
Nr   LogLevel  Time          Plugin     Revision  Message
448            03:14:31:618  Workspace  -         Start stopping ExecutionEngine
452            03:14:31:648  Workspace  -         ExecutionEngine successfully stopped
```

Info: 03:14:31:648: ExecutionEngine successfully stopped

Figure: 3DES in CryptTool 2

Bringing it all together

- We looked at *Data Encryption Standard*
- We also looked at the different variations of DES in CryptTool 2
- Next week: *Symmetric Encryption: AES*

Post-sessional work

- Create a CryptTool project which accepts a plaintext, and
  - First encrypts it using *any* classical cipher of your choosing
  - Then encrypts the resulting ciphertext with DES
  - Then gets the original plaintext back to its original form

Q & A

UNIVERSITY OF GLOUCESTERSHIRE