Week 4 Practical: *Advanced Encryption System (AES)*

Dr. Qublai Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

Recap

- Last week we looked at *Data Encryption System (DES)* and its different variants namely 3DES and SDES
- 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 *Advanced Encryption System (AES)* and *TwoFish*

AES Visualisation

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *AES Visualisation*
- In the Plaintext box, type in: `41 54 54 41 43 4b 20 41 54 20 4e 49 47 48 54 21` (hex for ATTACK AT MIDNIGHT!)
- In the Key box, type in: `59 45 4c 4c 4f 57 20 53 55 42 4d 41 52 49 4e 45` (hex for: *YELLOW SUBMARINE*)
- Finally click on the *Play* button to execute

AES Visualisation

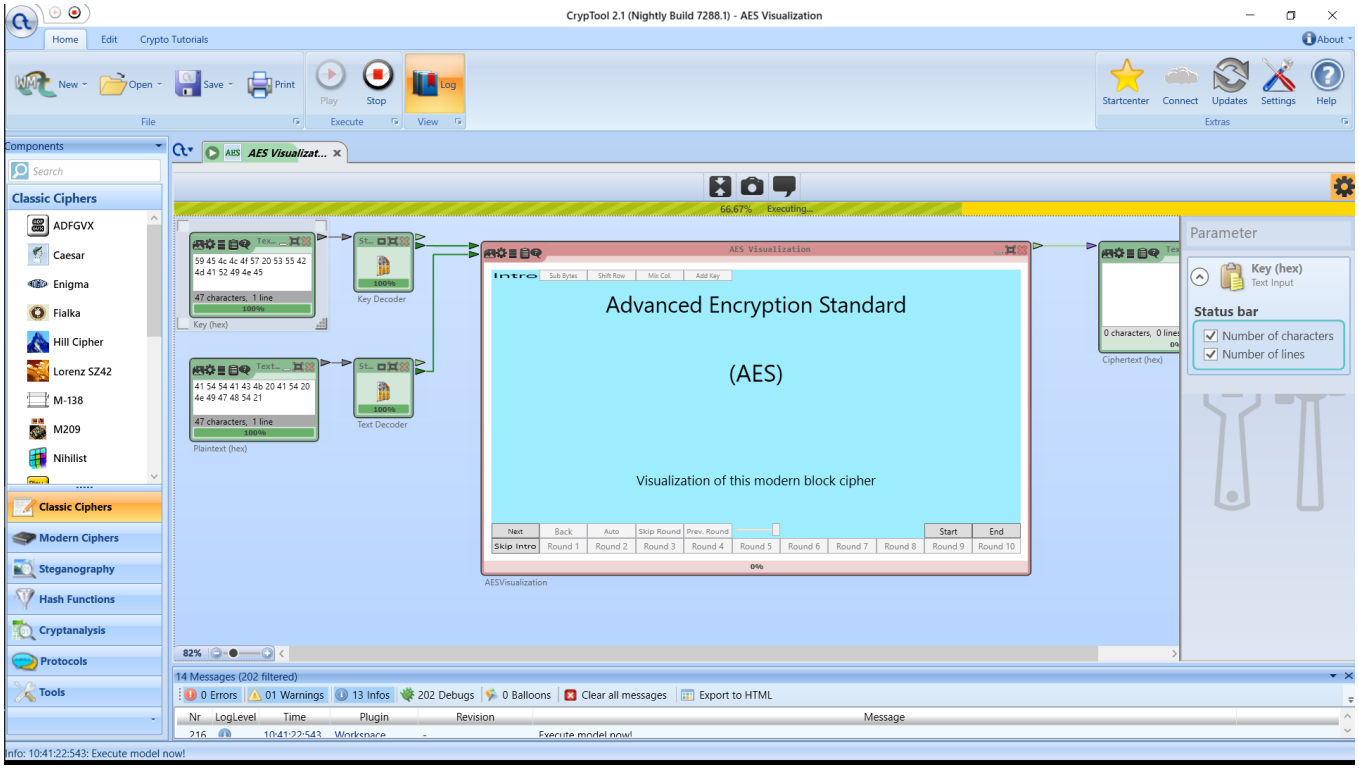

Figure: AES Visualisation

AES in CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *AES Cipher (Text Input)*
- In the Plaintext box, type in: `ATTACK AT MIDNIGHT!`
- In the Key box, type in: `59 45 4c 4c 4f 57 20 53 55 42 4d 41 52 49 4e 45` (hex for: *YELLOW SUBMARINE*)
- Finally click on the *Play* button to execute

AES in CryptTool 2

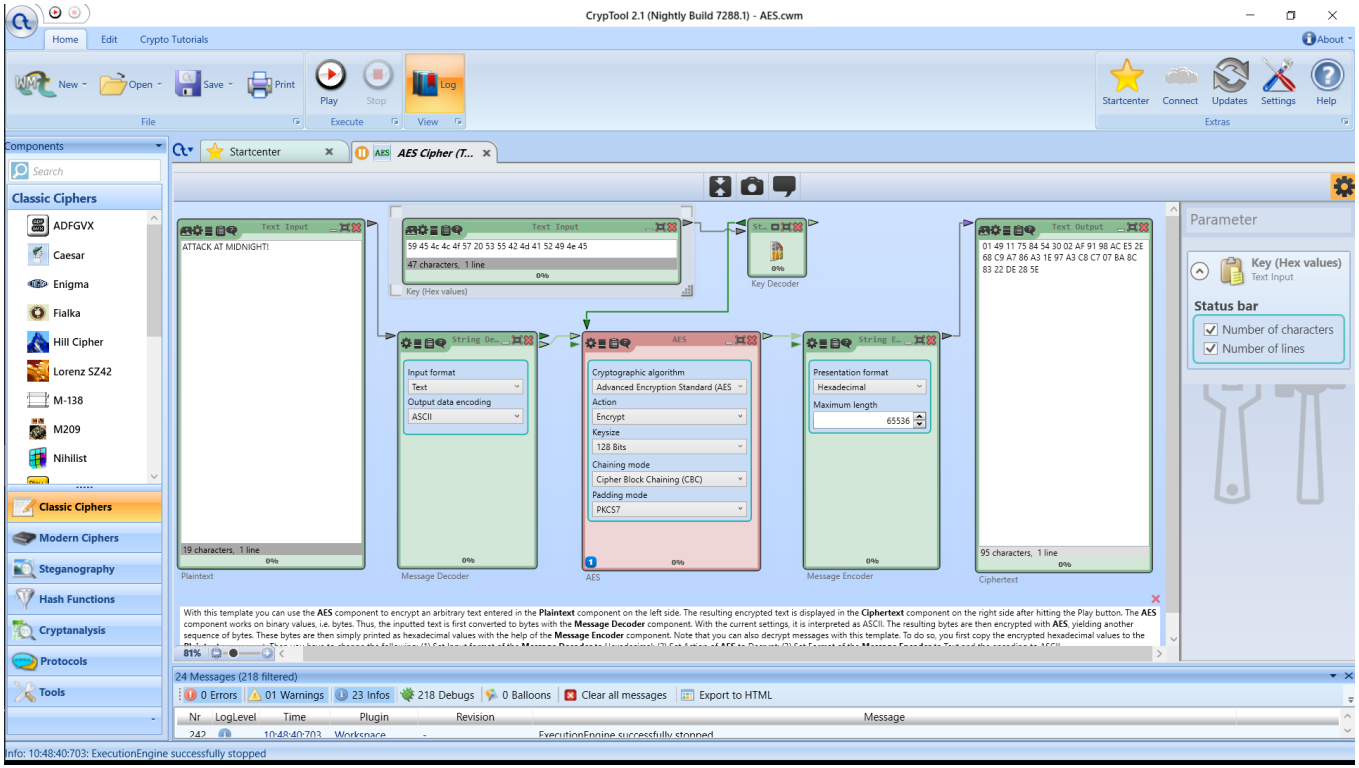

Figure: AES in CryptTool 2

AES/P in CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *AES (ECB) with PKCS#5*
- In the Plaintext box, type in: `ROSES ARE RED`
- In the Key box, type in: `GOLLUM`
- Finally click on the *Play* button to execute

AES/P in CrypTool 2

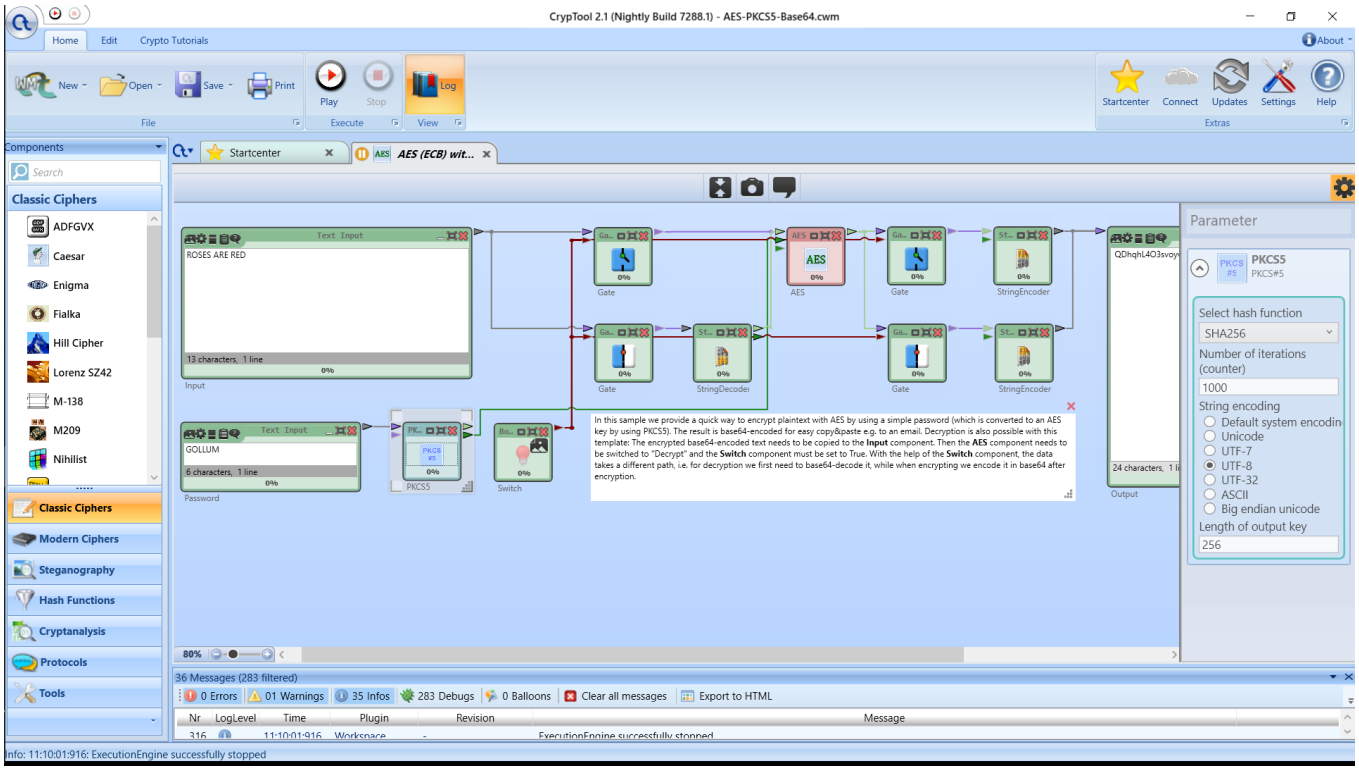

Figure: AES/P in CrypTool 2

TwoFish on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Modern* and then select *Symmetric*
- Next click *TwoFish Cipher*
- In the Plaintext box, type in: `ROSES ARE RED`
- In the Key box, type in: `47 4f 4c 4c 55 4d` (hex for: *GOLLUM*)
- Finally click on the *Play* button to execute

TwoFish on CryptTool 2

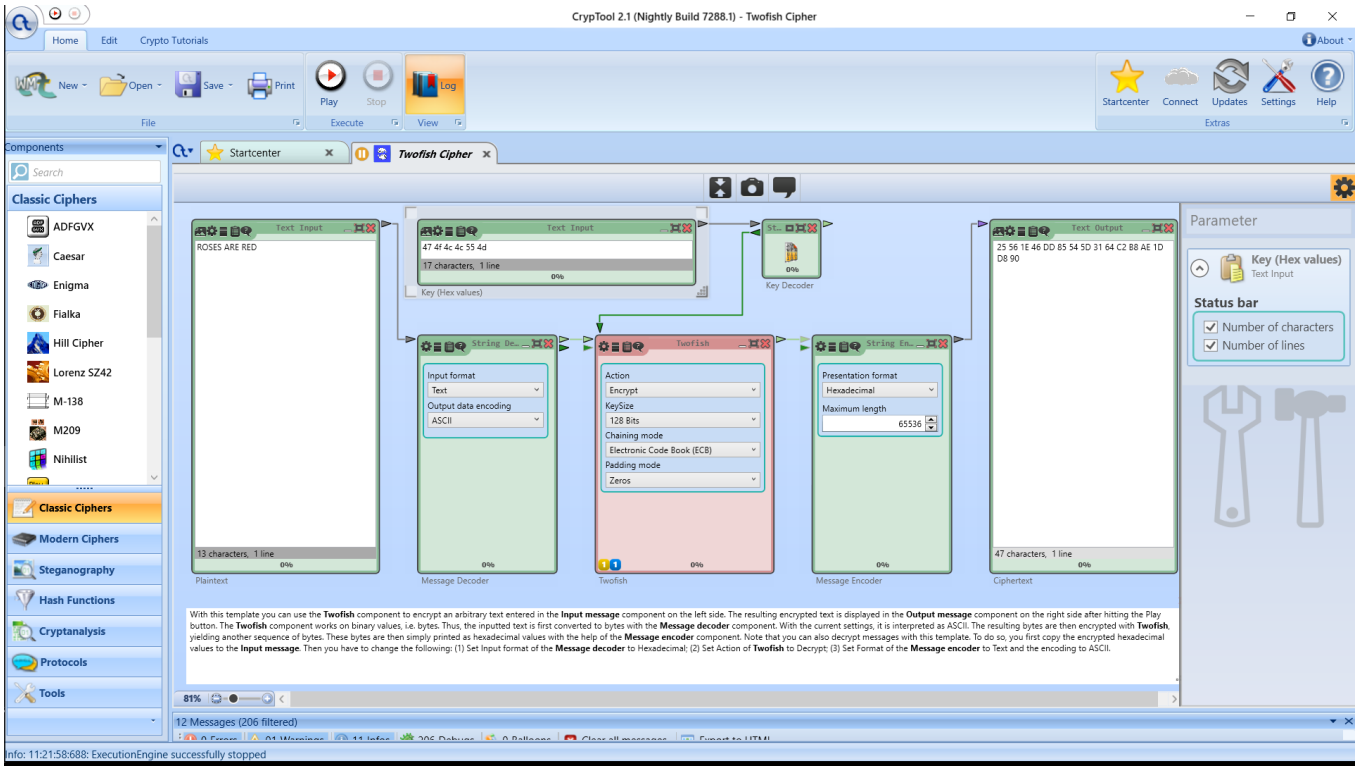

Figure: TwoFish in CryptTool 2

UNIVERSITY OF GLOUCESTERSHIRE

Bringing it all together

- We looked at *Advanced Encryption Standard (AES)* and *TwoFish*
- We also looked at the different variants of AES in CryptTool 2
- Next week: *Hashing*

Post-sessional work

- Create a CryptTool project which accepts a plaintext, and
  - First encrypts it using *DES*
  - Then encrypts the resulting ciphertext with AES
  - Then gets the original plaintext back to its original form

Q & A