Computer Security Course 2016-2017 **جامعة عين شمس**

Fourth Year Students [CSYS – CS - IS] **كلية الحاسبات و المعلومات**

Security Package

1- Required Algorithms in Security Package 2016/2017

Requirement	Serial	Algorithm	Input	
			Plaintext	**Key**
Mandatory - **Encryption** - **Decryption** - **Cryptanalysis**	1	General Ceaser.	Text	integer
	2	Monoalphabetic.	Text	Text
	3	Auto key vigenere.	Text	Text
	4	Repeating key Vigenere.	Text	Text
	5	PlayFair. [Cryptanalysis is Bonus]	Text	Text
	6	Hill Cipher.	Text OR Numbers	Text OR Numbers 2X2 OR 3X3
	7	Rail Fence of depth Level n.	Text	Integer (n)
	8	Columnar	Text	Integers
Choose one - **Encryption** - **Decryption**	9	DES. And 3-DES	Text OR HEX	Text OR HEX
	10	Multiplicative Inverse using Extended Euclid's.	Integers (No., Base)	
		AES.	Text OR HEX	Text OR HEX
Choose one	11	RC4.	Text OR HEX	Text OR HEX
	12	RSA.	Integers (p, q, M, e)	
Mandatory	13	Diffie-Hellman key exchange.	Integers (q, α, Xa, Xb)	
[Bonus]	14	MD5	TEXT	

2- Logistics:

- This Package is a team work task.
- All the group members MUST be from the same department
- Final Delivery will be scheduled on practical exams week.
- Registration Form (https://goo.gl/NNnHTJ).
- Registration deadline 25 February 2017.

Prof.Dr. Mohamed Hashem
Hanan Yousry – Yomna Mohsen – Hana Ibrahim – Donia Gamal

3- How to use the template code:

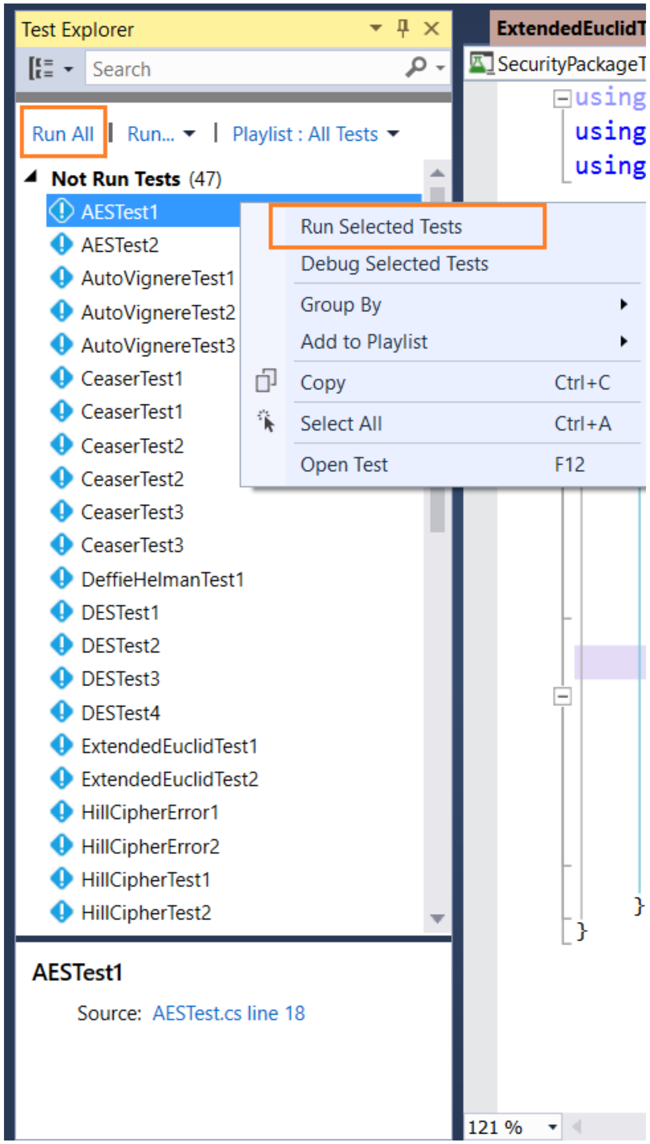
- You can get the package from here (https://bitbucket.org/Hanan_Hindy/fcissecuritypackagetemplate/branch/2017) or from the Dropbox folder (https://www.dropbox.com/sh/djxm2ae75de58lb/AAA9LFFhKcsI6lVwdoQLVCHUa?dl=0) .

- The solution you have consist of 2 projects:
  1- "SecurityLibrary": a dll project in which you'll write all your code.
  2- "SecurityPackageTest": a unit test project that you'll use to test your project.

- The "SecurityLibrary" project consists of a class for each algorithm. You have to **remove the thrown exception** and write your code in the correct place. Feel free to add the functions you need, you just need to keep the signature of these functions as they are:

```
public string Encrypt(string plainText, int key)
public string Decrypt(string cipherText, int key)
public int Analyse(string plainText, string cipherText)
```

- To test your code:
  1- Build the solution.
  2- Open test explorer (Test -> Windows -> Test explorer)


Test Explorer
Search
Run All
Run...
Playlist : All Tests
Not Run Tests (47)
AESTest1
AESTest2
AutoVignereTest1
AutoVignereTest2
AutoVignereTest3
CeaserTest1
CeaserTest1
CeaserTest2
CeaserTest2
CeaserTest3
CeaserTest3
DeffieHelmanTest1
DESTest1
DESTest2
DESTest3
DESTest4
ExtendedEuclidTest1
ExtendedEuclidTest2
HillCipherError1
HillCipherError2
HillCipherTest1
HillCipherTest2
AESTest1
Source: AESTest.cs line 18
Run Selected Tests
Debug Selected Tests
Group By
Add to Playlist
Copy Ctrl+C
Select All Ctrl+A
Open Test F12
ExtendedEuclidT
SecurityPackageT
using
using
using
121 %

3- If you want to run:
   a. All tests → "Run all"
   b. A specific test → right click, Run selected test
   c. The tests of a specific algorithm → open the test class of this algorithm, right click, run tests

4- For algorithms 9-14:
   a. Go to the test file of the algorithms you chose and remove `[Ignore]` from the class.

5- Additional test cases will be added, so make sure you're coding the algorithms correctly.