National College of Ireland

SECURITY FUNDAMENTALS & DEVELOPMENT

WEEK 3: CRYPTOGRAPHY

Kamil Mahajan
kmahajan@staff.ncirl.ie

AGENDA

- Group Presentations
- Crypto challenge

GROUP PRESENTATIONS

GROUP PRESENTATIONS

- Presenters:
  - –Approach the microphone so that everybody can hear you well
  - –Try to keep a good pace
  - –Watch your time
- Audience:
  - –Be respectful with your classmates and keep quiet during their presentation
  - –Engage with the topic presented


CAPTURE THE FLAG (CTF)
A Gamification of Cybersecurity Learning

CTF – CRYPTO CHALLENGE

Instructions: Given the clues in the question, infer the encryption algorithm involved and solve the challenge.

1) Of Caesar, my Caesar [3]

Ciphertext: lfdphlvdzlfrqtxhuhg

Plaintext=

2) hsabtA

Ciphertext: ZGYZHSRHHRNKOVYFGVZHBGLYIVZP

Plaintext=

3) Rail Fence Cipher (Encryption). Key =3

Special Instructions: Remove spaces when encrypting, do not use nulls. Alphabet: "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

Plaintext: Run away now

Ciphertext =

4) Rail Fence Cipher (Decryption), Key =3

Special Instructions: Remove any nulls that have been used

Alphabet: "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

Ciphertext: WSLDHTHUDEOAOWX

Plaintext: =

5) Another easy one (Vigenère)

Ciphertext: wqceagvmwgia

Plaintext=

CTF – CRYPTO CHALLENGE

Instructions:

Complete the table. What is the hash for the following Strings?

Use this link: http://asecuritysite.com/encryption/md5

Id	String	Algorithm	Hash
	Hello	MD5	8B1A9953C4611296A827A BF8C47804D7
6	hello	MD5	
7	goodbye	SHA-256	
8	This is my favorite subject	SHA-256	
9	d131dd02c5e6eec4693d9a0698aff95c2fcab5**8**712467eab4004583eb8fb7f8955ad340609f4b3028 3e4888325**7**1415a085125e8f7cdc99fd91dbd**f**280373c5bd8823e3156348f5bae6dacd436c919c6d d53e2**b**487da03fd02396306d248cda0e99f33420f577ee8ce54b67080**a**80d1ec69821bcb6a88393 96f965**2**b6ff72a70	MD5 Hex input	
10	d131dd02c5e6eec4693d9a0698aff95c2fcab5**0**712467eab4004583eb8fb7f8955ad340609f4b3028 3e4888325**f**1415a085125e8f7cdc99fd91dbd**7**280373c5bd8823e3156348f5bae6dacd436c919c6d d53e2**3**487da03fd02396306d248cda0e99f33420f577ee8ce54b6708**2**80d1ec69821bcb6a88393 96f965**a**b6ff72a70	MD5 Hex input	