**2022/2023 3010 Computer Security Semester 2**

**Week 11 Tutorial**

**Authentication/Password/Hash/Block & Stream cipher/RNG**

1. Is it always a bad idea to write down your password? Is there a way to do it more safely?
2. (a) Verify the computational complexity of these 3 entries: 10 character lower case alphanumeric, 9 character alphanumeric, 8 character printable keyboard characters in slide 16 of the Password Slides. What do you notice?

(b) The fastest Software Password crackers has cracking speed of up to 16 million passwords per sec (take it as 2^24) on a 3GHz PC. Estimate the time taken to compute cracking time of

(i) 10 numeric characters passwords

(ii) 8 character lower case alphanumeric passwords

(iii) 8 character alphanumeric passwords

(iv) 8 character all 95 printable characters passwords

1. Suppose that a certain email system uses hash of time when document is encrypted & emailed together. Example: time 20220203073000 means(3 February 2022 7:30:00)

* Alice encryption software works as follow:
* It uses 256-bit AES-encryption.
* Key used is 256-bit key, namely SHA256(Date & Time of email).
* When Alice use this encrypted email document and want to send to Bob, system looks at the time, then perform SHA256(Date & Time of email) and use this as 256-bit key for AES.
* Bob downloaded document into his pc. One day his pc is hacked and this document is in hands of hacker. Assume that hacker knows encryption algorithm and hash function used but not the date and time when document is sent.
* (a) Explore if hacker has a chance to read this document.
* (b) What are the key lessons we can learn from this implementation of strong algorithm AES?

1. Why do we want to use slow hash for password hashing?



1. Why do we need 256-bit hash length instead of 128-bit length to pair with AES-128?
2. Explain why a long codeword such as hippopotamus is not secure for use in Vignere cipher
3. Keystream of {0,1} generated by pseudo-random number generators will be periodic. Secure keystream must necessary have long period. Show that even with extremely long period, some keystreams may not be suitable for use to generate encryption keys.
4. Explain why for CTR mode in block cipher encryption, your counter values must all be distinct to be secure.
5. If the hash reflected on the web page of download coincides with your computed hash, does it always mean the files have not been tampered with, assuming the hash used is a real secured hash?