### **3413ICT Network Security**

|  |
| --- |
| **Workshop 1**  **Part 1 – Reviewing the lecture slides, answer the following questions**   1. Discuss different types of attacks against a cipher. Different types of attacks against a cypher include the following: 1. Brute Force attacks 2. Active attacks to gain information about a cypher such as breaking into an e-mail account go find a key. This also include passive attacks such as sniffing a network. 2. What is a brute-force attack? Brute force attack is when someone tries to break an algorithm by trying all key combinations in hopes of producing plaintext. 3. Discuss the following:    * Computer Security: generic name for the collection of tools, designed to protect data and to thwart hackers    * Network Security: measures to protect data in networked systems    * Internet Security: measures to protect data during their transmission over the Internet 4. Explain the following terms in relation to information transmission.   Authentication: assurance that the communicating entity is the one claimed  Integrity: assurance that data received is as sent by an authorized entity  Non-repudiation: protection against denial by one of the parties in a communication   1. Suppose you and your partner have agreed to transfer some private information using a simple bit-level encryption - XOR operation. Explain how this can be achieved. |
| **Part 2 – Challenge Exercise**  In this exercise, you explore various Internet resources and learn about some common types of computer security incidents. You need a computer with a Web browser and access to the Internet.   1. Using your Web browser and favourite search engine, explore the Internet and find sites that contain descriptions of computer security threats. To get started, you may look at the following sites:    * 1. *The site of the Computer Emergency Response Team (CERT).*      2. *http://www.sans.org*      3. *The site of Anti****-****Phishing Working Group* (APWG)      4. *http://www.microsoft.com/security* 2. Give one example of an attack that violates the confidentiality goal of computer security.    * Snooping from another workstation    * Use external router link to enter & snoop    * Monitor and/or modify data traffic 3. Give one example of an attack that violates the integrity goal of computer security.   Modification: Such as changing data in a file that a user is not authorized to view. Changing the content of a message being sent on the network.   1. Give one example of an attack that violates the availability goal of computer system.   Interruption attack such as ‘Denial of service’. |

**Part 3 – Hands-on Exercise**

**CrypTool** is an [open source](http://en.wikipedia.org/wiki/Open_source)  [learning](http://en.wikipedia.org/wiki/E-learning) tool illustrating [cryptographic concepts](http://en.wikipedia.org/wiki/Cryptology), which was originally developed by German companies and universities. It is now an [open source](http://en.wikipedia.org/wiki/Open_source) project. More than 40 people worldwide contribute regularly to the project. Its role is to make users aware of how cryptography can help against network security threats and to explain the underlying concepts of cryptology. CrypTool provides a graphical interface, including analytic tools and cryptographic [algorithms](http://en.wikipedia.org/wiki/Algorithm). [Classical ciphers](http://en.wikipedia.org/wiki/Classical_cipher) are available alongside [asymmetric cryptography](http://en.wikipedia.org/wiki/Public-key_cryptography) such as [RSA](http://en.wikipedia.org/wiki/RSA), [elliptic curve cryptography](http://en.wikipedia.org/wiki/Elliptic_curve_cryptography), [digital signatures](http://en.wikipedia.org/wiki/Digital_signature) and [Diffie-Hellman key exchange](http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange), many of which are visualized by animations. It also contains an animated tutorial on the basic mathematical techniques for cryptography (such as primes and elementary [number theory](http://en.wikipedia.org/wiki/Number_theory)).

Download the latest version of CrypTool (a copy will be provided by your tutor in the workshop classes, if needed). Install the software. We will use this software to complete hands-on exercises in the following days.