IT.law@hku.hk - class 4

- Public Key Infrastructure
- Electronic Transactions Ordinance

1

Basic Terminology

- What is encryption?
- What is an algorithm?

2

- Single key or symmetric systems
- problem with this single key system

- Two-Key or asymmetric systems
- Public Key cryptography or asymmetric cryptosystem

3

- Cryptanalysis and key lengths

  - Breaking codes:
  - obtain the private key from a holder
  - find a weakness in the algorithm
  - brute force

  - Ease of brute force cryptanalysis is a function of the length of the key

4

- **Definitions of key terms in the Electronic Transactions Ordinance**
- **Electronic Transactions Ordinance, s 2:**
- **"asymmetric cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for generating a digital signature and a public key to verify the digital signature**

- technology specific approach

5

- **Example: Sending a message using asymmetric cryptosystem**

  - **Sender - Recipient**
  - **– encryption of the content of a document**

- **Which key should be used?**
- **Whose key should be used?**

6

- For encryption of the content of a message:
- To send an encrypted message - Use the recipient's public key
- To decrypt an encrypted message - Use the recipient's private key

7

- What is the definition of a "digital signature" under the Electronic Transactions Ordinance?
- Under the Electronic Transactions Ordinance, a digital signature does not just mean a signature in a digital format.
- Example: you scan a copy of your handwritten signature and store it in the format of a computer file – is this a "digital signature" under the Electronic Transactions Ordinance?

8

- Electronic Transactions Ordinance, s 2:
- “electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record

9

- Electronic Transactions Ordinance s 2
- "digital signature", in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine-
- (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and
- (b) whether the initial electronic record has been altered since the transformation was generated;

10

- Practically, how do you “sign” a digital signature?
- A digital signature is a block of data that is generated from a message prior to its despatch, and is appended to it.

11

- The function of a hash algorithm:
- **Electronic Transactions Ordinance, s 2:**
- **"hash function" means an algorithm mapping or transforming one sequence of bits into another, generally smaller, set as the hash result, such that-**
- **(a) a record yields the same hash result every time the algorithm is executed using the same record as input;**
- **(b) it is computationally not feasible for a record to be derived or reconstituted from the hash result produced by the algorithm; and**
- **c) it is computationally not feasible that 2 records can be found to produce the same hash result using the algorithm**

12

- The sender:
- a “hash result” is created using a one-way hash algorithm; and
- this “hash result” is encrypted with the sender's private key.

- The recipient:
- re-creates the hash result from the message that they receive,
- uses the sender's public key to decrypt the digital signature that they received appended to the message itself, and compares the two results to see if they are identical.

13

content integrity

authentication

non-repudiability of messages

14

- **What keys are used in this process?**
- **To send an encrypted digital signature - Use the sender's Private key**
- **Decrypt an encrypted digital signature (and authenticate the sender) - Use the sender's Public key**

15

- Hong Kong Electronic Transactions Ordinance (passed on January 7, 2000)
  - objective of fostering an environment conducive to the development of electronic commerce
  - grants the same legal status to electronic records and digital signatures as that of paper-based records and manual signatures
  - provides for the establishment of a voluntary licensing system, in the form of government recognition for certification authorities

16

- Is there a general requirement under Hong Kong law that contracts need to be in writing?

17

– **Under the Electronic Transactions Ordinance, a digital signature is only recognized if it is supported by a digital certificate issued by a Recognized Certification Authority (RCA).**

18

- Establishment of a Voluntary Recognition System of Certification Authorities (CA) and Creation of Recognized Certification Authorities (RCA)

- The Role of the Director of Information Technology Services
- power of recognition, revocation, suspension
- Code of Practice

19

- RCAs will be afforded significant limitations on its potential legal liabilities by the Electronic Transactions Ordinance - the RCAs may specify in their certificates 'reliance limits' which are set up as a cap on their legal liabilities

  - Unless intentional misrepresentation, negligent or reckless misrepresentation

20