School of Digital Media and Infocomm Technology

### ST2504 Applied Cryptography

1. a) What is a digital signature?

**A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.**

1. State three objectives of a digital signature.

* **It verifies author, date and time of signature**
* **It authenticates message contents - receiver’s compare hash value**
* **Can be verified by third parties to resolve disputes**

2. a) What is a direct digital signature?

* **It involves only sender and receiver**
* **It assumes receiver has sender’s public-key**
* **The digital signature is created by the sender signing the entire message or hash with private-key**
* **The security depends on the sender’s private key**

b) State two possible pitfalls of direct digital signature.

* **Sender may deny sending the message and claim that the private key was stolen**
* **Private key may be stolen at time T and the opponent can then send a message signed and stamped with a time before or equal to time T**

3. a) What is an arbitrated digital signature?

**It involves the use of arbiter A, which is a trusted party to validate any signed message i.e. Docusign**

b) Briefly describe how it works.

* **First, the arbiter validates any signed message**
* **Subsequently stamp it and send to recipient**
* **It requires suitable level of trust in arbiter**
* **It can be implemented with either private or public-key algorithms**
* **The arbiter may or may not see message**

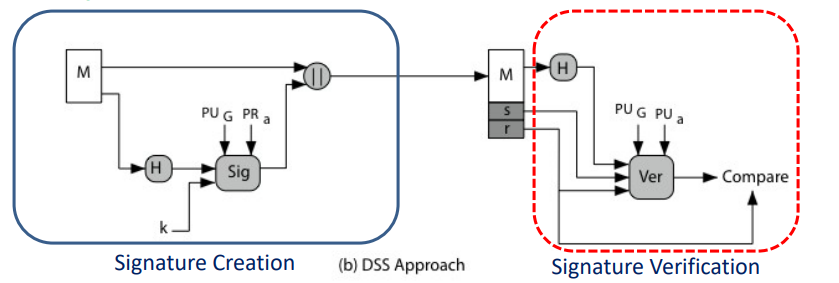
4. With the aid of a diagram, briefly describe the characteristics of the Digital Signature Scheme (DSS).

**DSS algorithm uses the message hash, global public values (PUG), private key (PRa) and random (k) to create a 2 part signature (s,r).**

**This is verified by computing a function of the message hash, public key (Pua), r and s, and comparing the result with r.**

* **DSS creates a 320-bit signature with 512-1024 bit security (Key) - (discrete logarithm)**
* **It is smaller and faster than RSA**
* **Uses SHA hash algorithm**
* **DSS is a digital signature scheme that uses discrete logarithms**

**Several important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem has no efficient solution.**

****