PUBLIC KEY CRYPTOGRAPHY

Seminar 6

1. Use the RSA digital signature scheme with Alice having the public key $(n, e) = (1517, 7)$ and the private key $d = 823$. Analyze the following actions:

(1) Alice sends the message "*Mathematics*" together with her digital signature of the ToyHash value of the message.

(2) Eve intercepts Alice's message and signature, changes the message into "*Informatics*", and sends it to Bob together with Alice's digital signature.

(3) Bob verifies Alice's signature and accepts the (changed) message from Alice.

2. Use the RSA digital signature scheme with Alice having the public key $(n, e) = (1517, 7)$ and the private key $d = 823$. Analyze the following actions:

(1) Alice sends the message "*Computer Science*" together with her digital signature of the ToyHash value of the message.

(2) Eve intercepts Alice's message and signature, finds a message having the same ToyHash value as the message "*Computer Science*", changes Alice's message with it, and sends it to Bob together with Alice's digital signature.

(3) Bob verifies Alice's signature and accepts the (changed) message from Alice.

3. Use the Rabin digital signature scheme with Alice having the public key $n = 1643$ and the private key $(p, q) = (31, 53)$. Analyze the following actions:

(1) Alice sends the message "*Mathematics*" together with her digital signature of the ToyHash value of the message.

(2) Eve intercepts Alice's message and signature, changes the message into "*Informatics*", and sends it to Bob together with Alice's digital signature.

(3) Bob verifies Alice's signature and accepts the (changed) message from Alice.

4. Use the ElGamal digital signature scheme with Alice having the public key $(p, g, g^a) = (2357, 2, 1185)$ and the private key $a = 1751$. Analyze the following actions:

(1) Alice sends the message "*Mathematics*" together with her digital signature of the ToyHash value of the message.

(2) Eve intercepts Alice's message and signature, changes the message into "*Informatics*", and sends it to Bob together with Alice's digital signature.

(3) Bob verifies Alice's signature and accepts the (changed) message from Alice.