JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.de

Prof. Dr. Kai Rannenberg
Welderufael B. Tesfay, MSc.
Ahmed S. Yesuf, MSc.

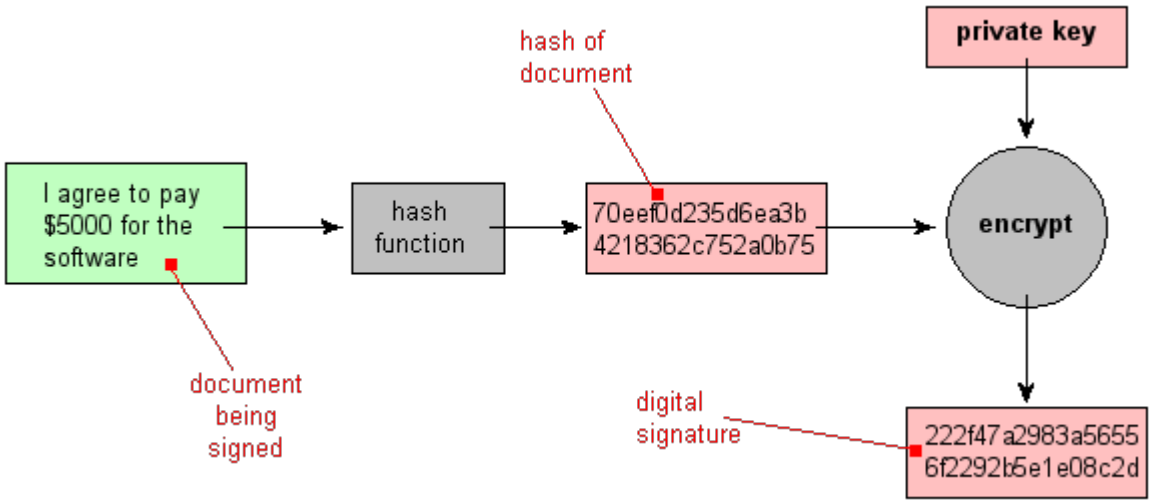
Telefon +49 (0)69-798 34706
Telefax +49 (0)69-798 35004
E-Mail sec@m-chair.de

Information and Communications Security
SS 16
Assignment 3
Cryptography

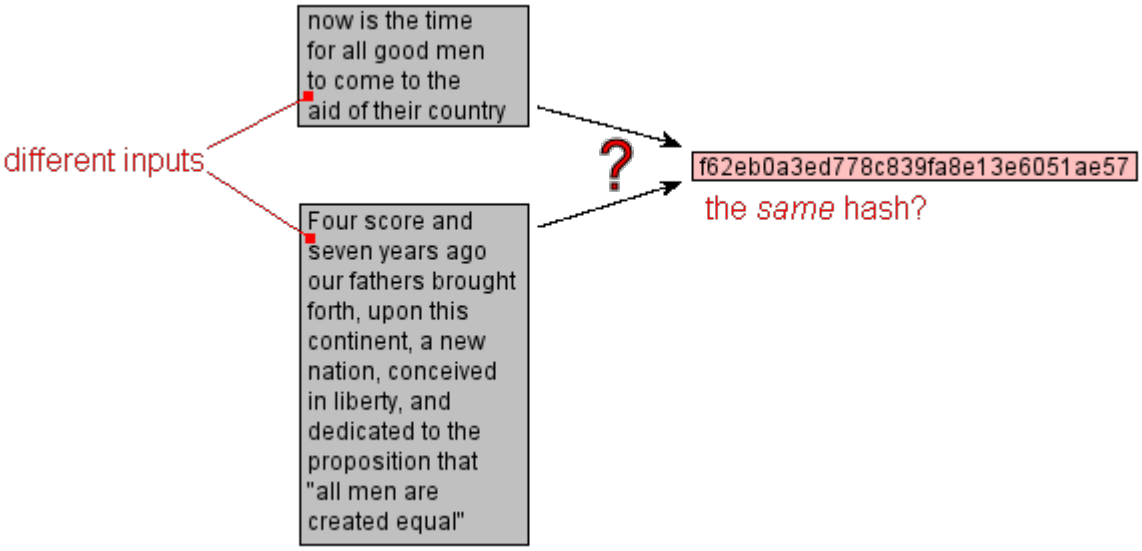
Study the following questions and prepare your answers before the **14th of June 2016.**

Exercise 1: (PGP)
Install PGP Email Desktop (trial version) or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to welderufael.tesfay@m-chair.de containing your newly created public key and a short summary of your experiences.
PGP can be downloaded from http://www.symantec.com/business/desktop-email.

Exercise 2: (Hash functions and signature systems)
The image below shows the steps of digitally signing a document. The sender receives the plain document and the digital signature.



Hash functions always produce a fixed size value, no matter how big the plain text is. For example, MD5 produces 128 bits. But if it is possible to represent every possible stream of data in 128 bits (16 bytes), then it seems obvious that there are many input streams that can produce the same hash value. When two inputs produce the same hash value, this is called collision (see Figure below).



Given a fixed message m1, if we cannot find in a practical way a different message m2 such that hash(m2) = hash(m1), then we say that this hash function is collision-resistant.

a) In the digital signature scheme, why do we produce the signature on the hash of the document and not on the document directly?
b) Why is it important that hash functions are collision-resistant?

Exercise 3: (Caesar)
Break the following ciphertext, given that the Caesar cipher was used to encrypt it:

NZIVSNCZB QA QV OMZUIVG

(Hint: Start by a permutation of the alphabet by 1, then 2, until 10, stop when the result makes sense in English.)

Exercise 4: Symmetric vs. asymmetric crypto

a) Describe differences between symmetric and asymmetric cryptosystems.

b) Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.

Exercise 5: Stream ciphers

a) What is a one-time pad (Vernam-code)?

b) Alice wants to encrypt the letter `A`, where the letter is given in ASCII code. The ASCII value for `A` is $65_{10} = 1000001_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext:

b1) 10100110
b2) 0011111
b3) 101010

c) Encrypt the message using Vernam code and using XOR as an encryption function and the key in b).