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
Ahmed S. Yesuf, MSc.

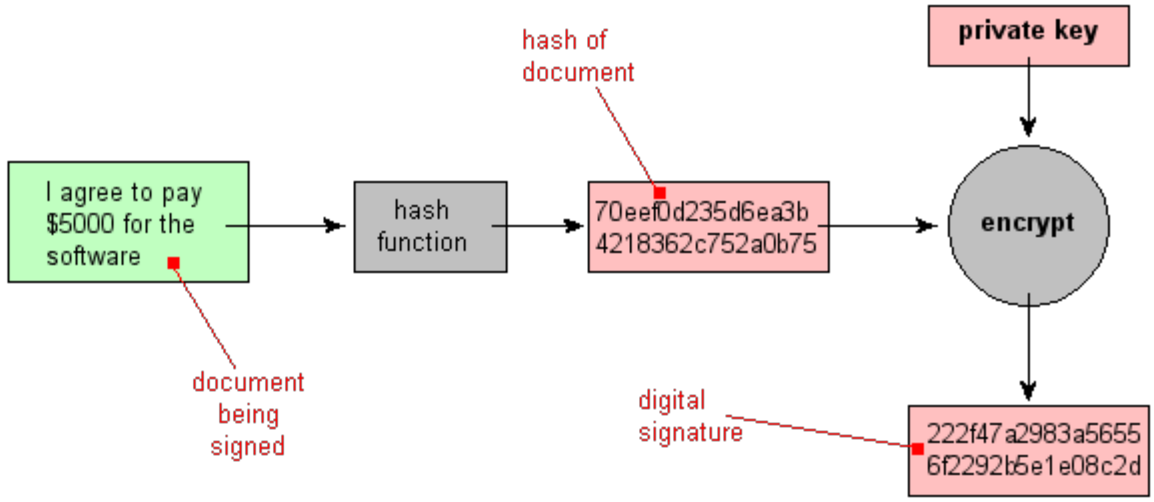
Telefon +49 (0)69-798 34706
Telefax +49 (0)69-798 35004
E-Mail sec@m-chair.de

Information and Communications Security WS 16/17 Assignment 4 Cryptography II

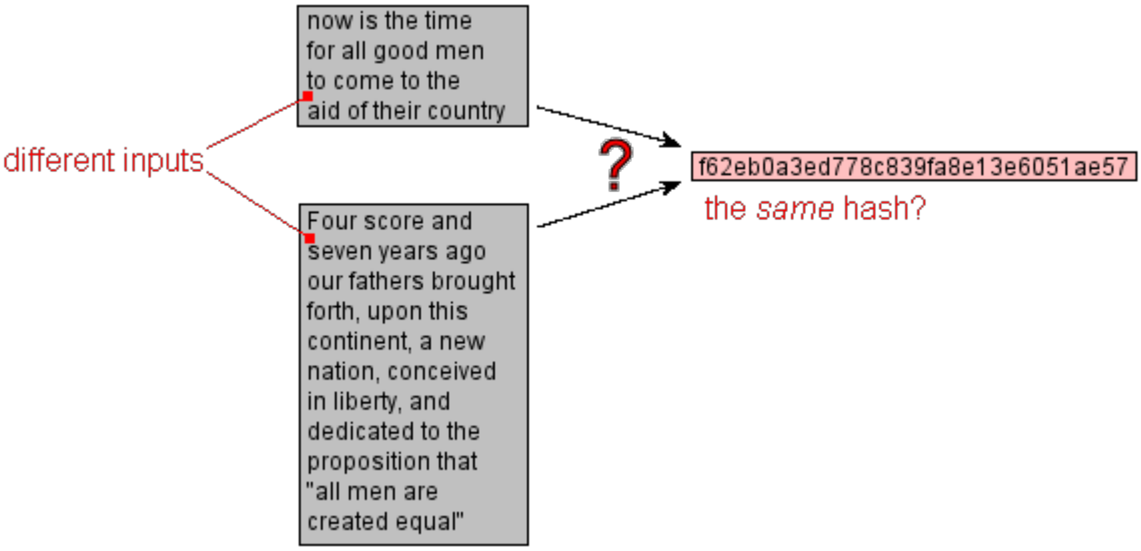
Study the following questions and prepare your answers before the **14th of December 2016.**

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 ahmed.yesuf@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 of document
private key
I agree to pay $5000 for the software
hash function
70eef0d235d6ea3b 4218362c752a0b75
encrypt
document being signed
digital signature
222f47a2983a5655 6f2292b5e1e08c2d

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).


now is the time for all good men to come to the aid of their country
different inputs
?
f62eb0a3ed778c839fa8e13e6051ae57
the *same* hash?
Four score and seven years ago our fathers brought forth, upon this continent, a new nation, conceived in liberty, and dedicated to the proposition that "all men are created equal"

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:

a) What is the difference between public key encryption and digital signature?
b) Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.