

Information and Communications Security WS 14/15 Assignment 3 Cryptography

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
M.Sc. Ahmed S. Yesuf
M.Sc. Fatbardh Veseli
M.Sc. Christopher Schmitz

Telefon +49 (0)69-798 34705
Telefax +49 (0)69-798 35004
E-Mail sec@m-chair.de

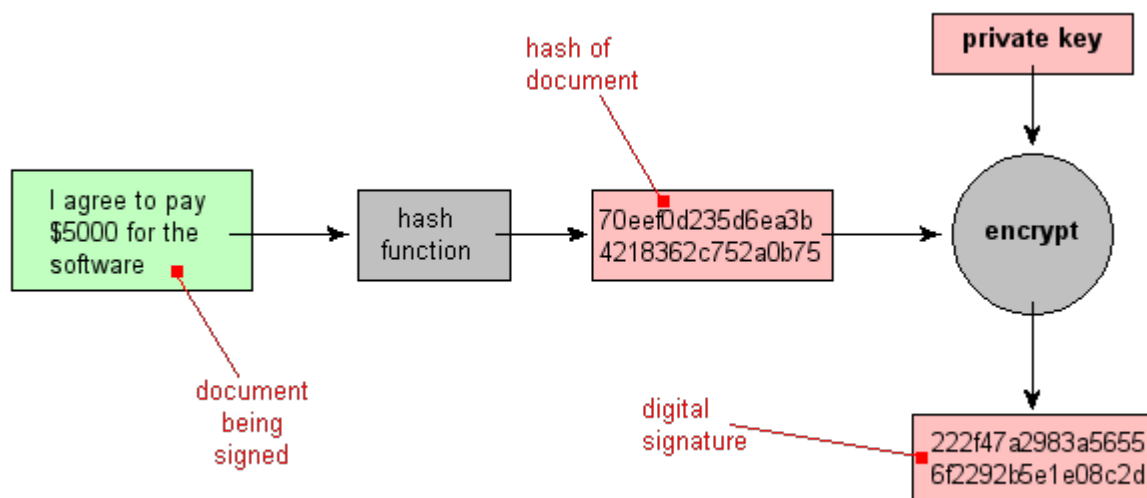
Study the following questions and prepare your answers before **3rd of Dec 2014**.

Exercise 1: (PGP)

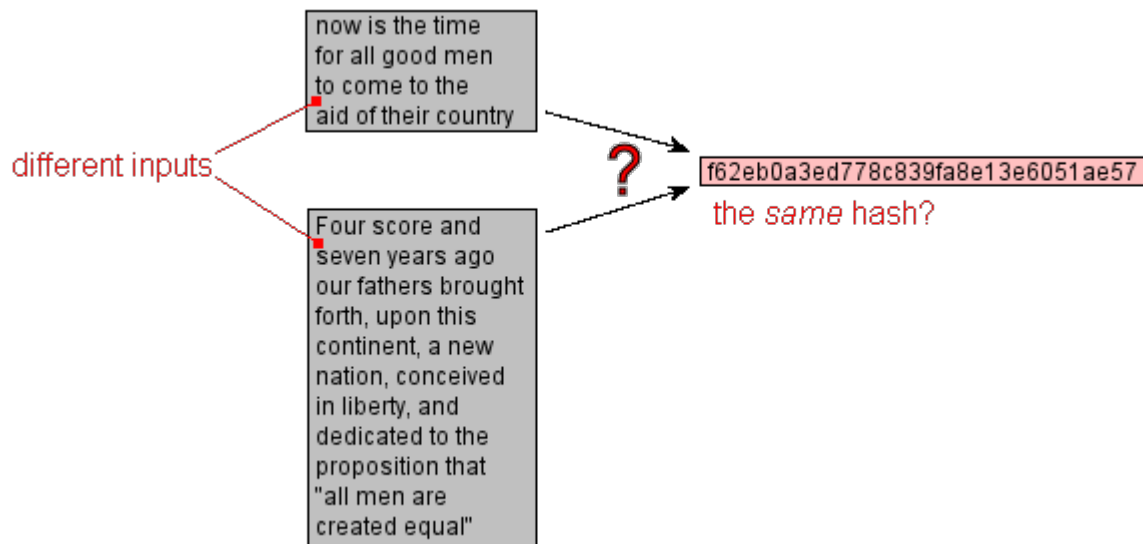
Install PGP Email Desktop (trial version) or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to ahmed.yesuf@m-chair.de containing your newly created public key and a short summary of your experiences. PGP can be downloaded from <http://www.symantec.com/business/desktop-email>

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 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 m_1 , if we cannot find in a practical way a different message m_2 such that $\text{hash}(m_2) = \text{hash}(m_1)$, then we say that this hash function is collision-resistant.

- In the digital signature scheme, why do we produce the signature on the hash of the document and not on the document directly (Hint: You need to do some research in http://en.wikipedia.org/wiki/Digital_signature)?
- 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 produce it:

NZIVSNCZB QA QV OMZUIVG

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

Exercise 4: (Misc)

- Describe differences between symmetric and asymmetric cryptosystems.
- Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.