Assignment 4 - Cryptography and Digital Signature

Information & Communication Security
(WS 2016/17)

Ahmed S. Yesuf (M.Sc.)

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

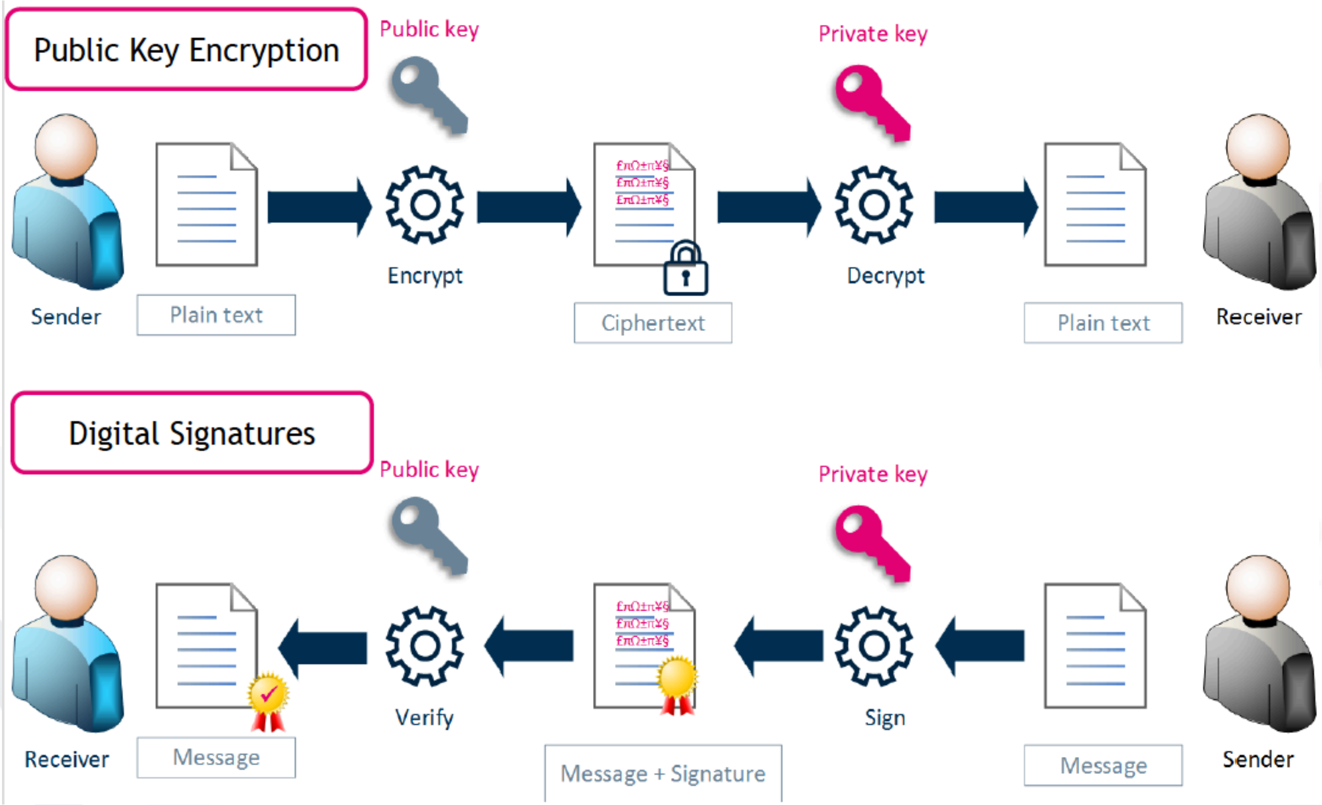
Exercise 3

a) What is the difference between public key encryption and digital signature?

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

Asymmetric Signature System

a) What is the difference between public key encryption and digital signature?



Digital Signatures

Definition: A digital signature is a construct that authenticates both origin and contents of a message in a manner that is provable to a third party.

[Bishop2005]

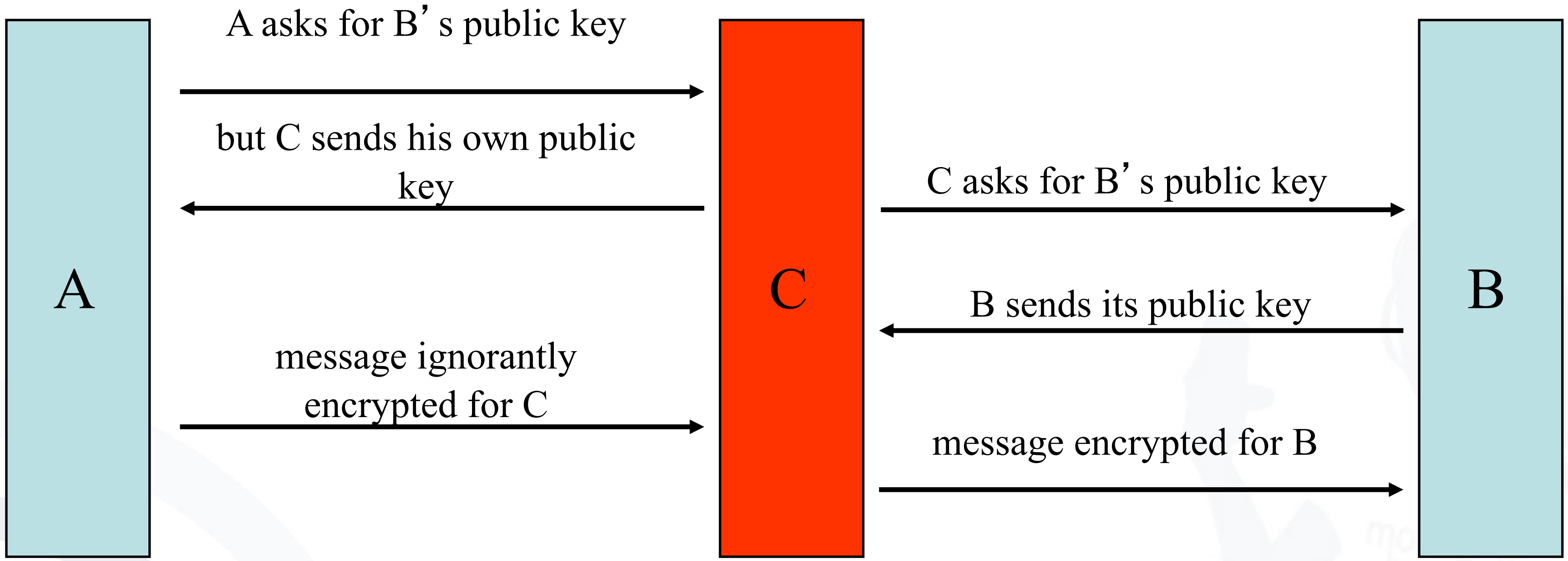
Asymmetric Signature system

Digital signatures	Public Key Encryption
The holder of the private key (sender) signs the message.	"Any one" can encrypt a message.
"Any one" can verify that a signature is valid.	Only the holder of the private key (receiver) can decrypt the message.

Exercise 3(b)

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

Exercise 3


A asks for B’s public key
but C sends his own public key
message ignorantly encrypted for C
A
C
B
C asks for B’s public key
B sends its public key
message encrypted for B

➲ Keys are certified: a 3rd person/institution confirms (with its digital signature) the affiliation of the public key to a person.

Certification of Public Keys

Three types of organization for certification systems (PKIs?):

- Central Certification Authority (CA)
  - A single CA, keys often integrated in checking software
  - Example: older versions of Netscape (CA = Verisign)
- Hierarchical certification system
  - CAs which in turn are certified by “higher” CA
  - Examples: PEM, TeleTrust, infrastructure according to Signature Law
- Web of Trust
  - Each owner of a key may serve as a CA.
  - Users have to assess certificates on their own.
  - Example: PGP (but with hierarchical overlay system)

Exercise 3: Misc

What are advantages and disadvantages of asymmetric crypto systems?

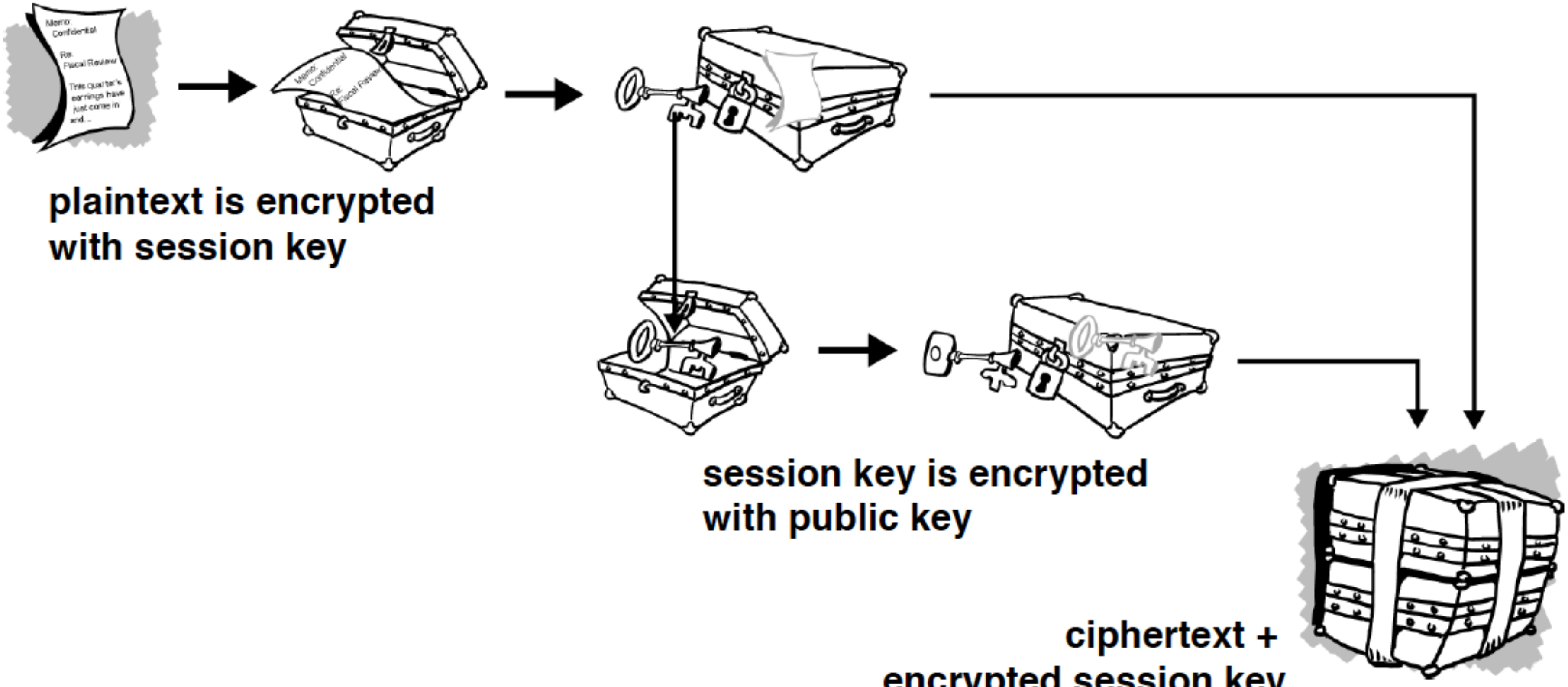
Advantages:

- No secret must be shared
- Only one key per endpoint

Disadvantages:

- Algorithms are very slow
- Man-in-the-middle-attack

Hybrid encryption: PGP Example Encryption

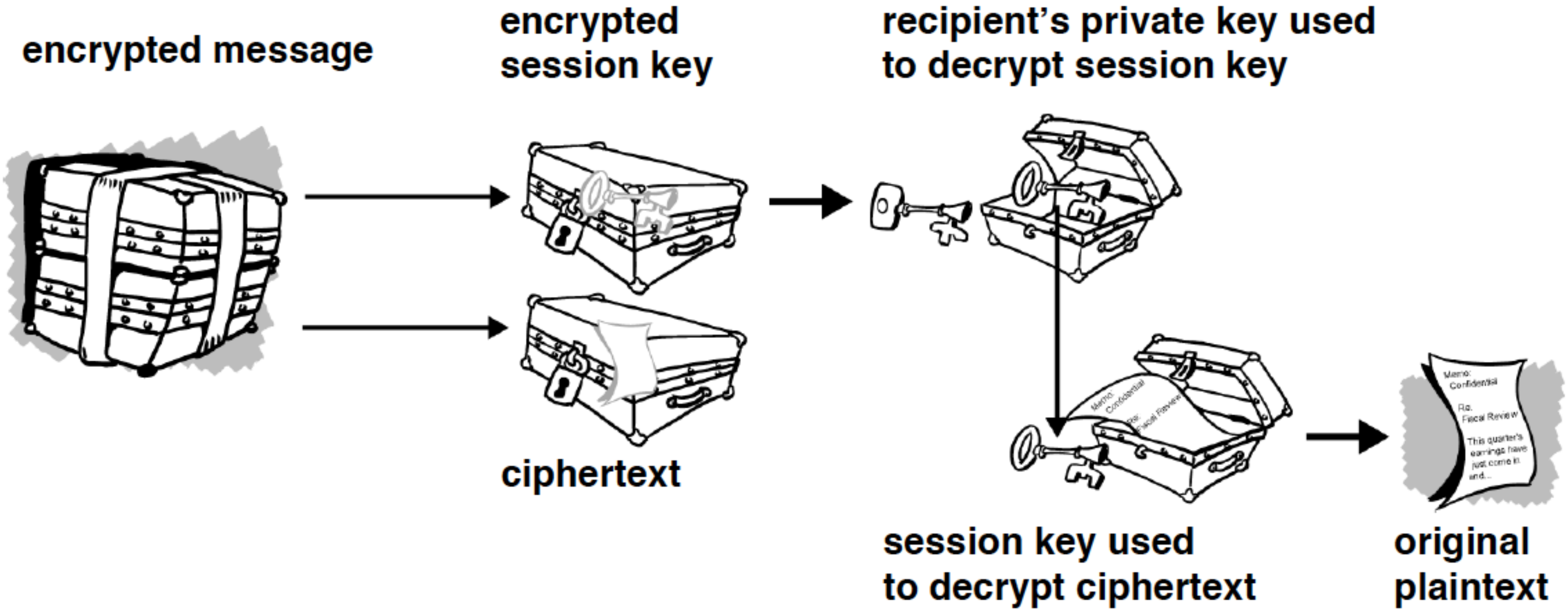


plaintext is encrypted with session key

session key is encrypted with public key

ciphertext + encrypted session key

PGP Decryption



encrypted message

encrypted session key

ciphertext

recipient's private key used to decrypt session key

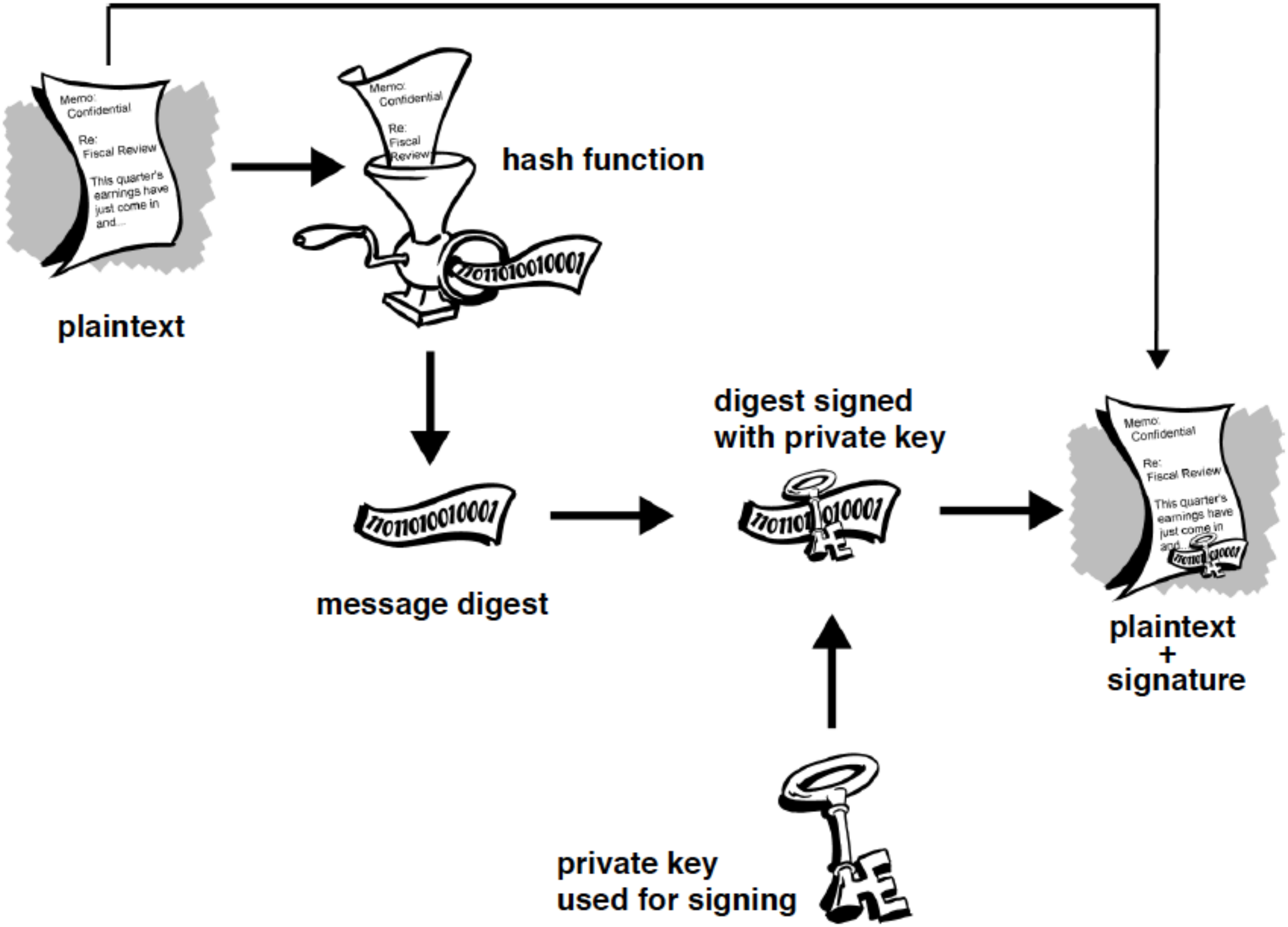
session key used to decrypt ciphertext

original plaintext

PGP example continued…

- Encryption offers
  - Confidentiality
- Digital Signatures offer
  - Authentication
  - Integrity

Digital Signatures

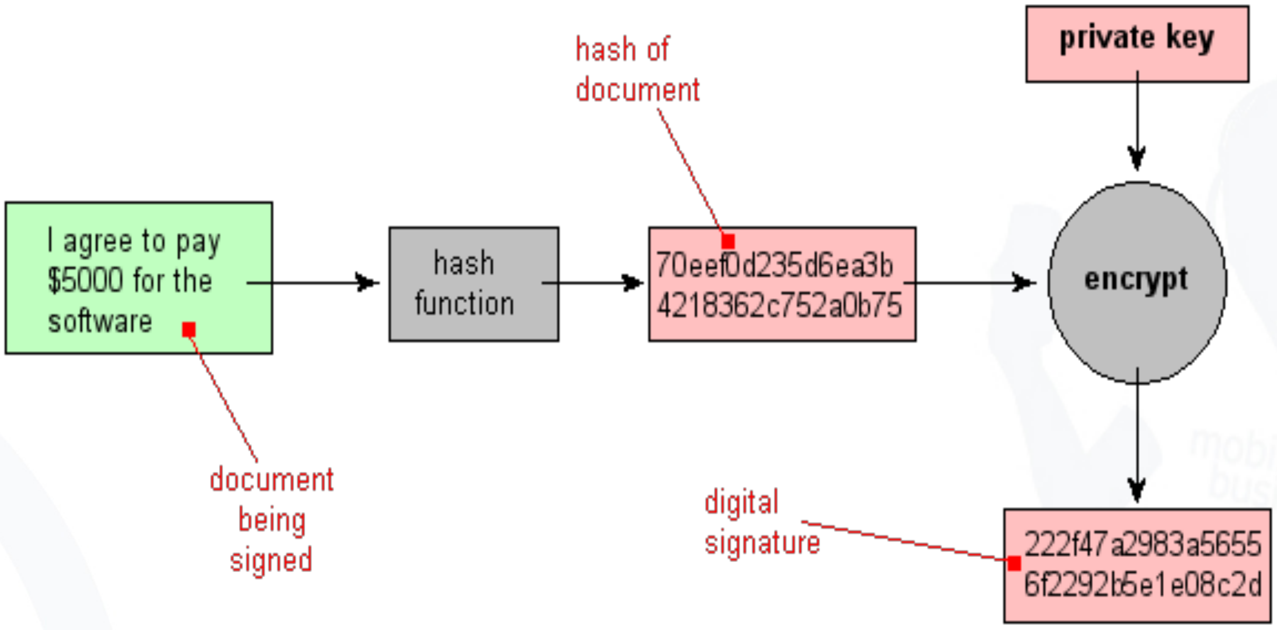


Exercise 1: PGP

- 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
  - Practical exercise, no solution required, check lecture notes for overview of PGP
  - Be careful to only send your public key
  - If you haven’t done this yet, try it, sending encrypted mail is useful, and we want you to be able to do it.

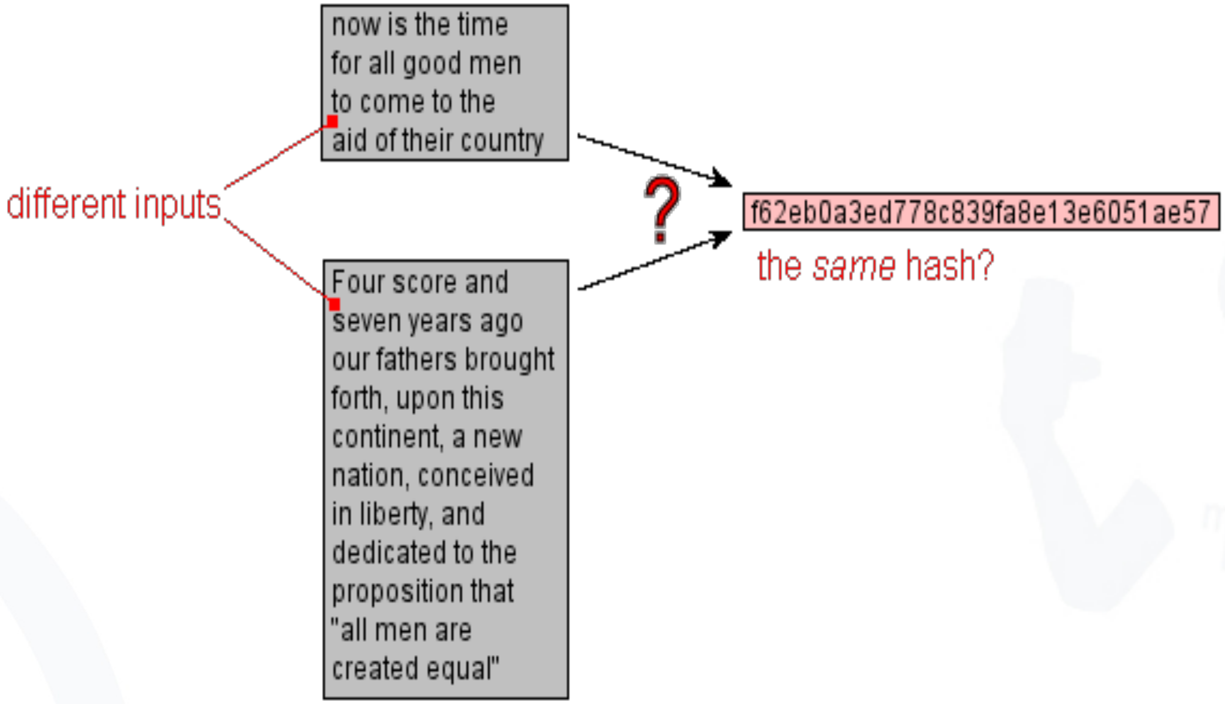
Exercise 2: Hash functions and signature systems

- 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

Exercise 2: Hash functions and Signature Systems (2)

- When two different inputs produce the same hash value - collision



now is the time for all good men to come to the aid of their country

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"

Exercise 2: Hash functions and Signature Systems (3)

- 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?

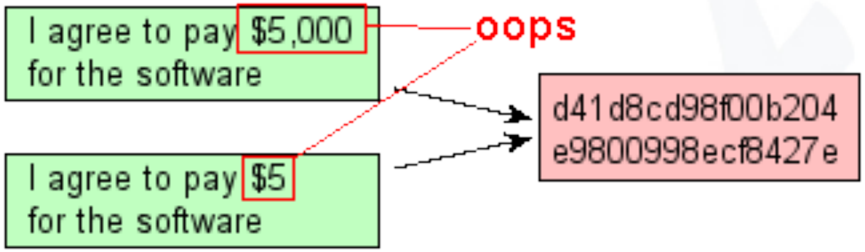
efficiency	integrity
The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.	Without the hash function, the text "to be signed" may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize if all the blocks are present and in the appropriate order.

Exercise 2: Hash functions and Signature Systems (4)

- 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*.

b. Why is it important that hash functions are collision-resistant?

- In some digital signature systems, a party attests to a document by publishing a public key signature on a hash of the document.
  - If it is possible to produce two documents with the same hash, an attacker could get a party to attest to one, and then claim that the party had attested to the other.
- Software version comparison. An attacker who could produce two files with the same hash could trick users into believing they had the same version of a file when they in fact did not.


I agree to pay $5,000 for the software
oops
d41d8cd98f00b204 e9800998ecf8427e
I agree to pay $5 for the software

Thank you!

- Questions: sec@m-chair.de