

## *Assignment 3 - Cryptography*

SEC 2011

Dr. Ioannis Krontiris

Chair of Mobile Business and Multilateral Security  
Goethe-Universität Frankfurt a. M.



## Exercise 3: Caesar Cipher

- Decrypt the following word, encrypted with the Caesar cipher:

JYFWAVNYHWOF

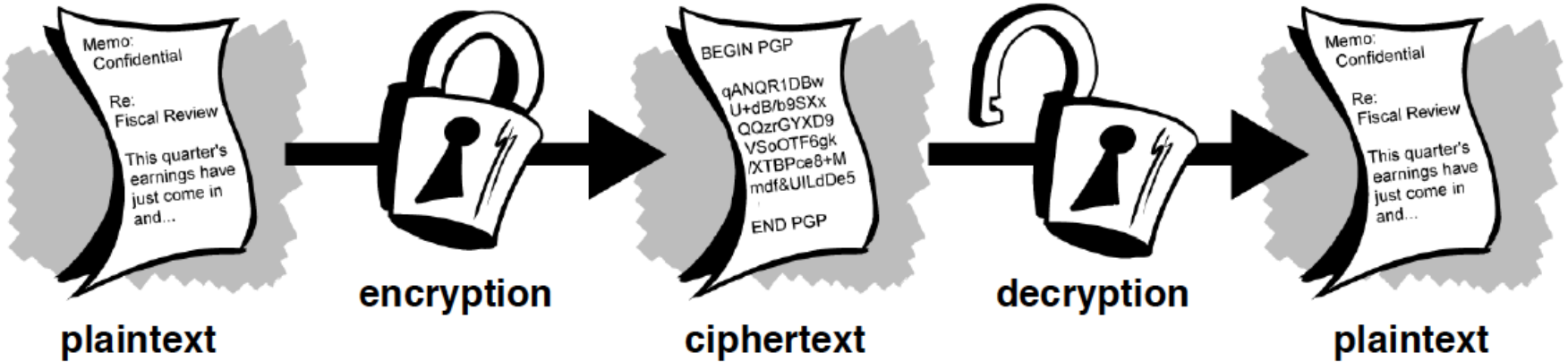
- Let's try:

Key	J	Y	F	W	A	V	N	Y	H	W	O	F
1	I	X	E	V	Z	U	M	X	G	V	N	E
2	H	W	D	U	Y	T	L	W	F	U	M	D
3	G	V	C	T	X	S	K	V	E	T	L	C
4	F	U	B	S	W	R	J	U	D	S	K	B
5	E	T	A	R	V	Q	I	T	C	R	J	A
6	D	S	Z	Q	U	P	H	S	B	Q	I	Z
7	C	R	Y	P	T	O	G	R	A	P	H	Y

- Very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space ( $n=26$ )
- Therefore, the encryption is very easy and fast to compromise.

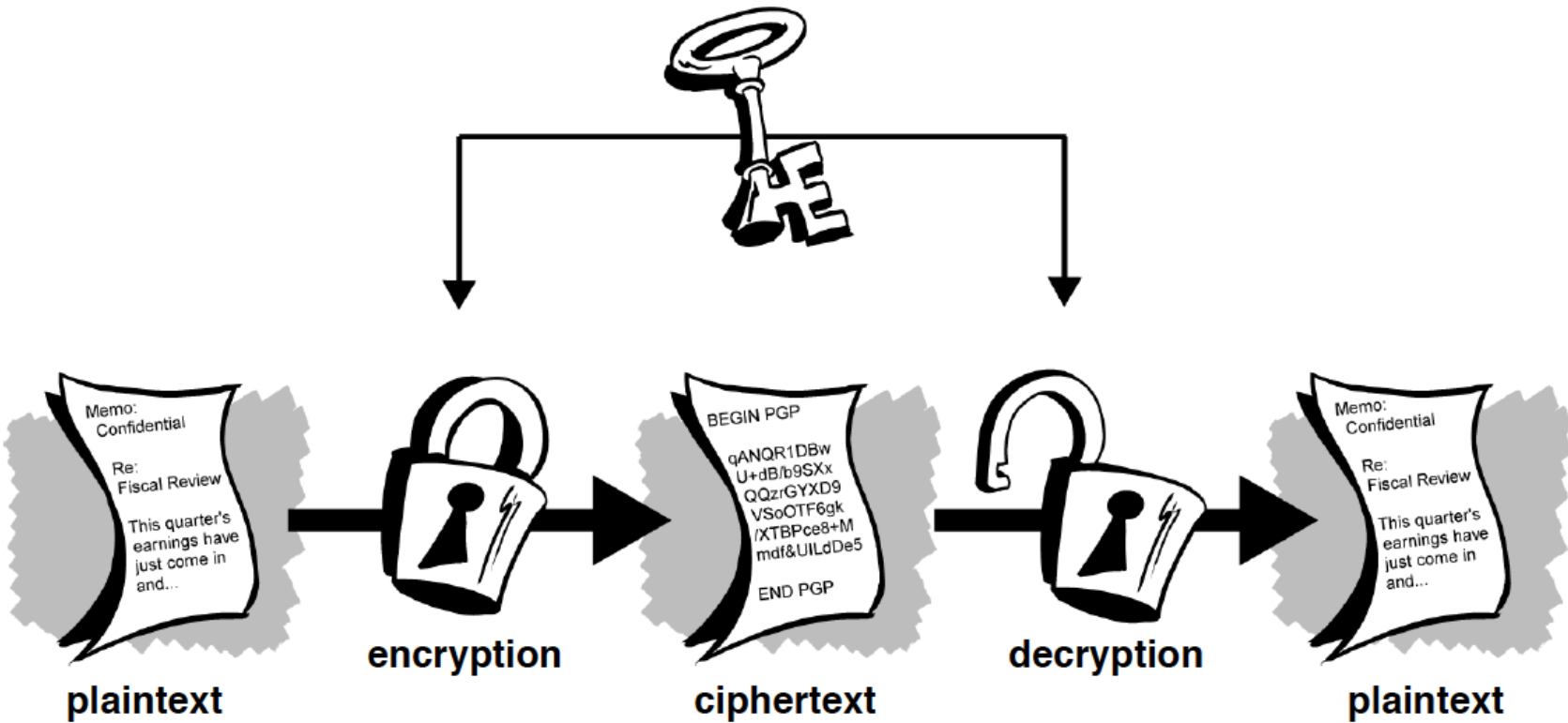
- Install GNUPG or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to [ioannis.krontiris@m-chair.net](mailto:ioannis.krontiris@m-chair.net) containing your newly created public key and a short summary of your experiences.
  - Practical exercise, no solution here, check lecture notes for overview of PGP
  - Be careful to only send your public key
  - You can also send your existing public key, but in this case be extra careful
  - If you haven't done this yet, try it, sending encrypted mail is useful, and we want you to be able to do it.

# Encryption - Decryption



<http://www.pgpi.org/doc/guide/6.5/en/intro/>

# Shared-key Cryptography

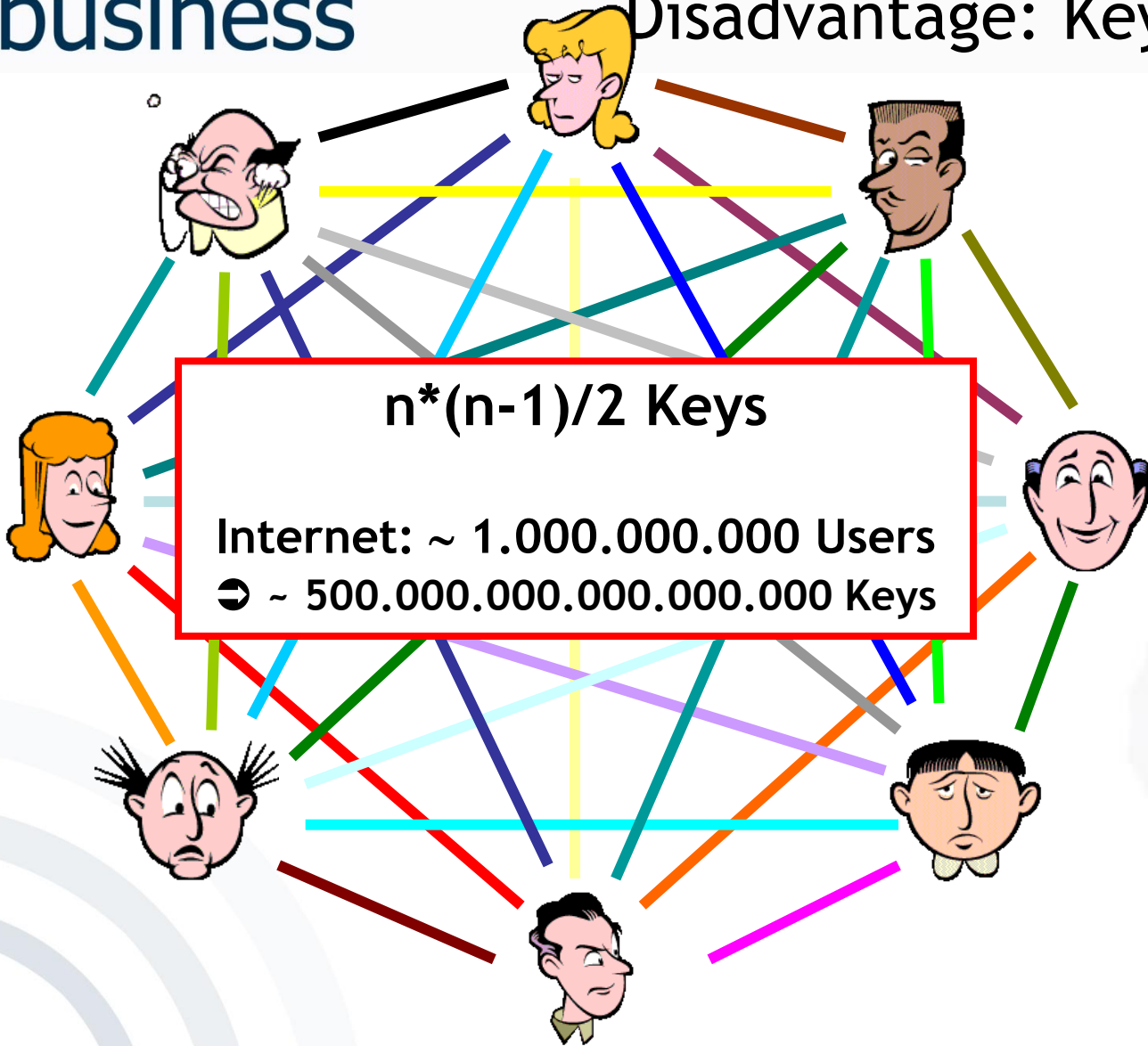


## Advantage: Algorithms are very fast

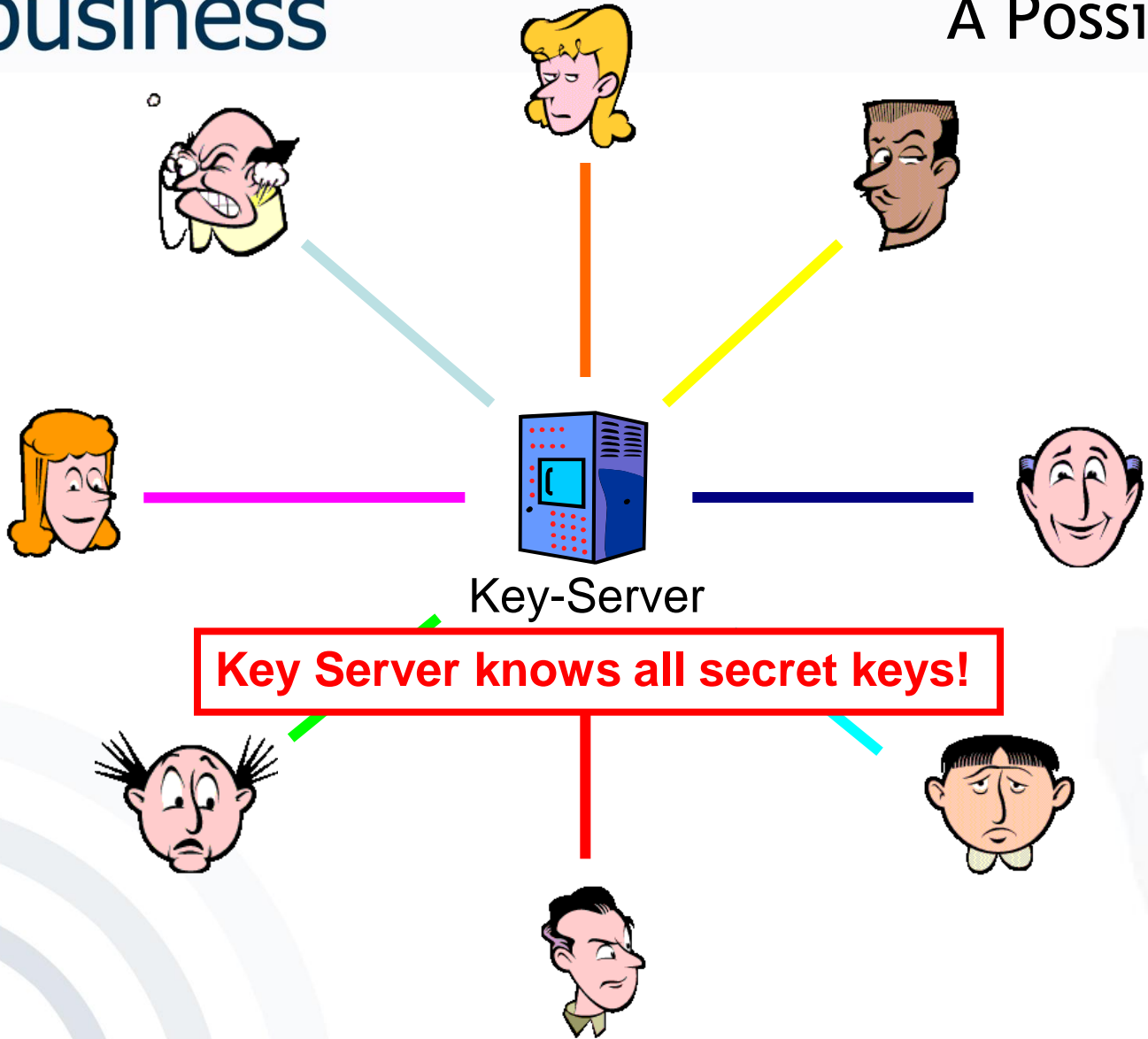
Algorithm	Performance*
RC6	138 ms
AES	173 ms
SERPENT	200 ms
IDEA	288 ms
MARS	394 ms
TWOFISH	697 ms
DES-ede	726 ms

\*) Encryption of 1 MB-blocks with an Athlon 1GHz processor

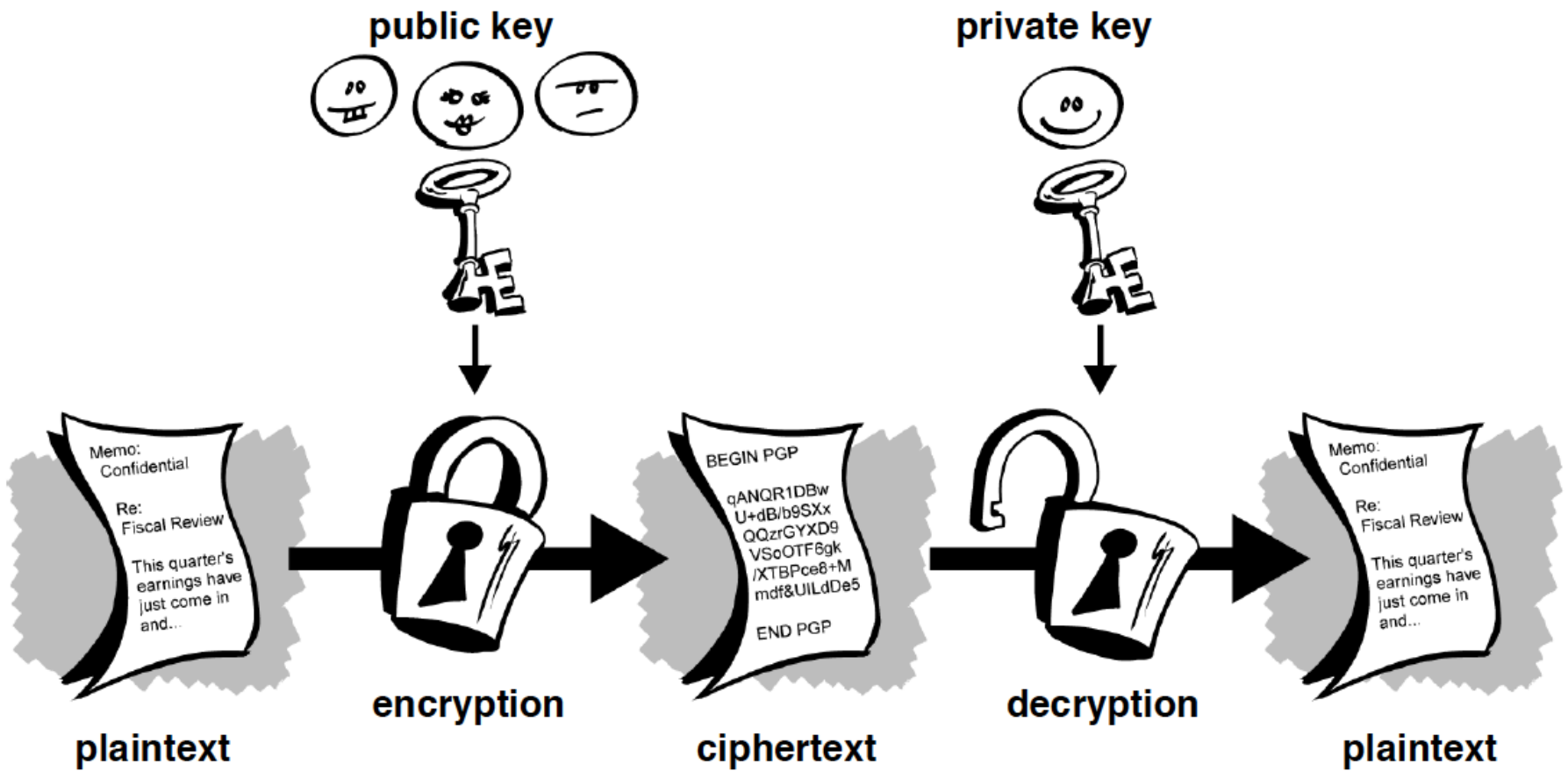
Disadvantage: Key Distribution



[adopted from J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]



# Public-key cryptography



Algorithm	Performance*
El Gamal	1826 s
RSA	16 s

**Disadvantage:** Complex operations  
with very big numbers

➔ **Algorithms are very slow**

\*) Encryption of 1 MB-blocks with an Athlon 1GHz processor

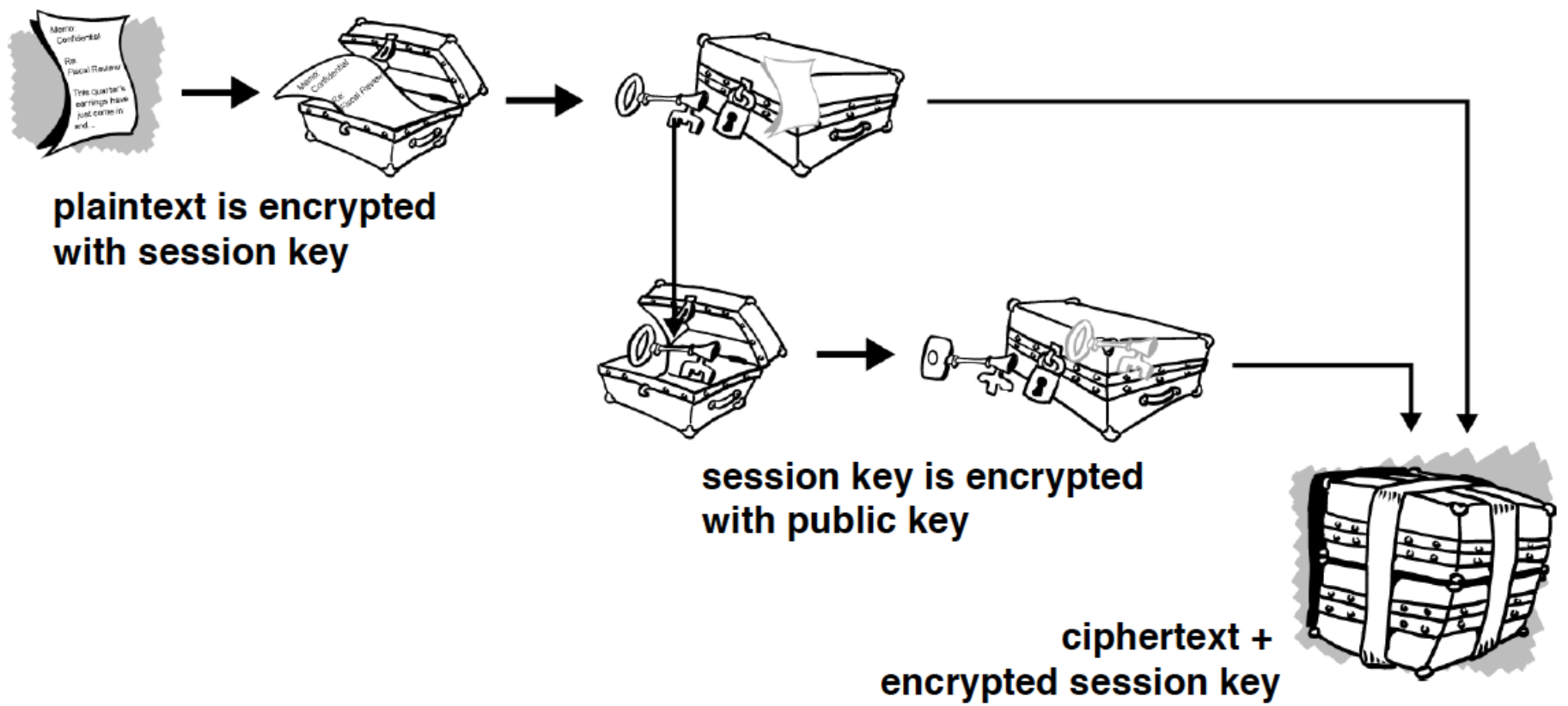
c. What are advantages and disadvantages of asymmetric encryption/decryption?

Advantages:

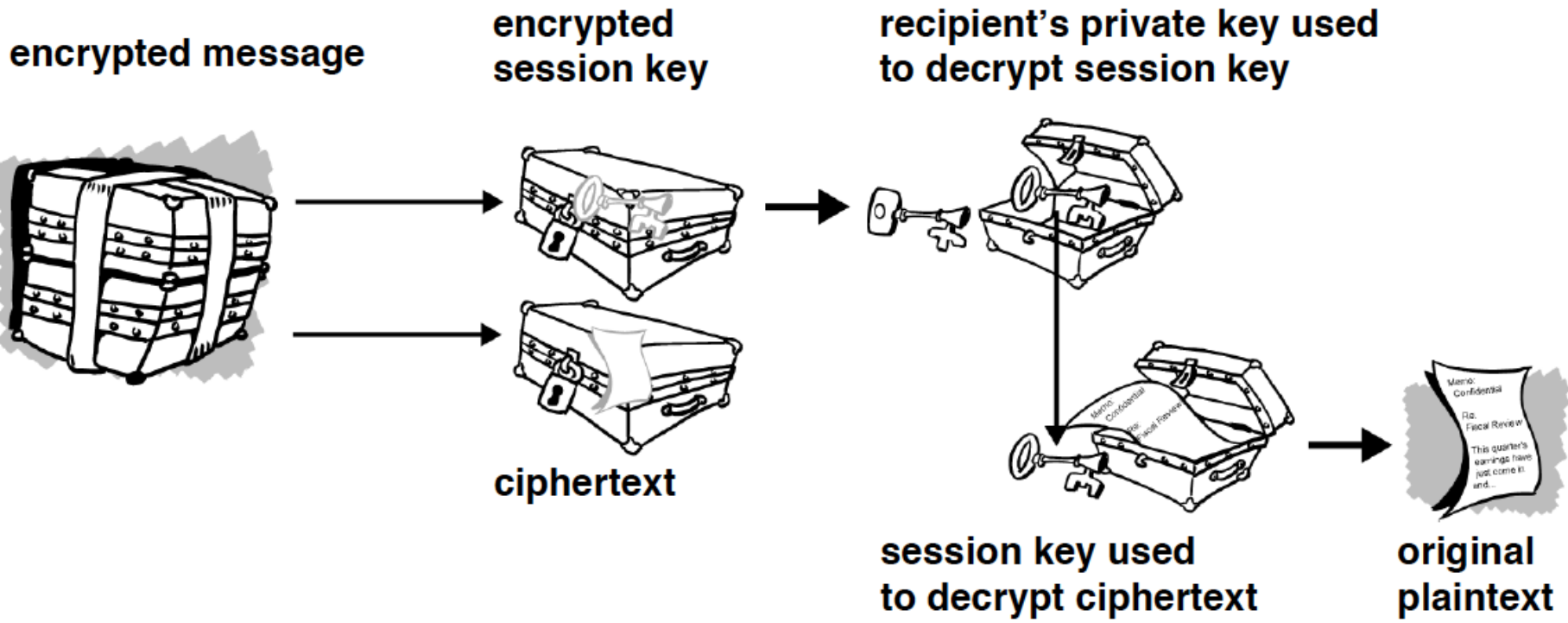
- No secret must be shared
- Only one key per endpoint

Disadvantages:

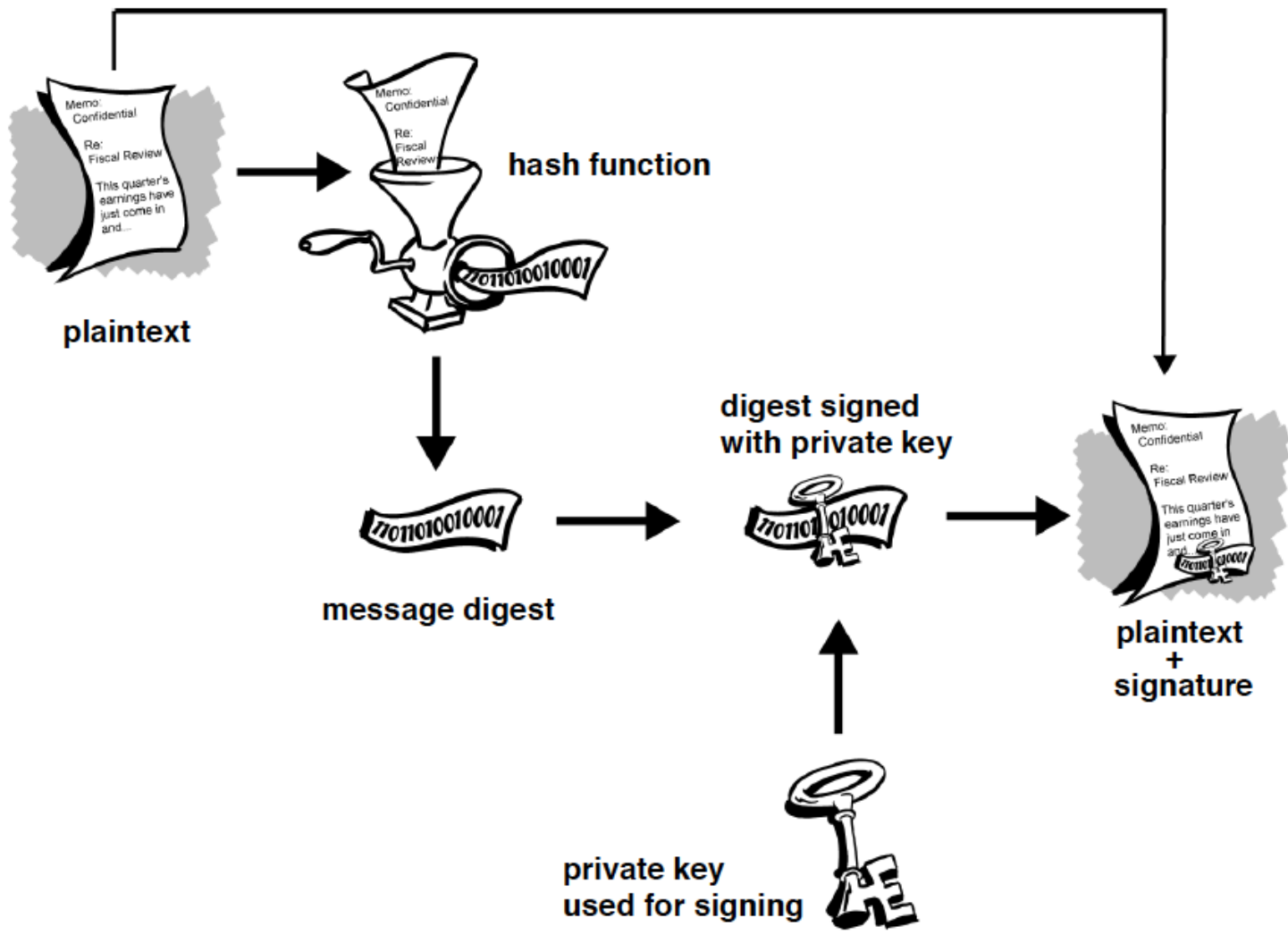
- Algorithms are very slow
- Man-in-the-middle-attack

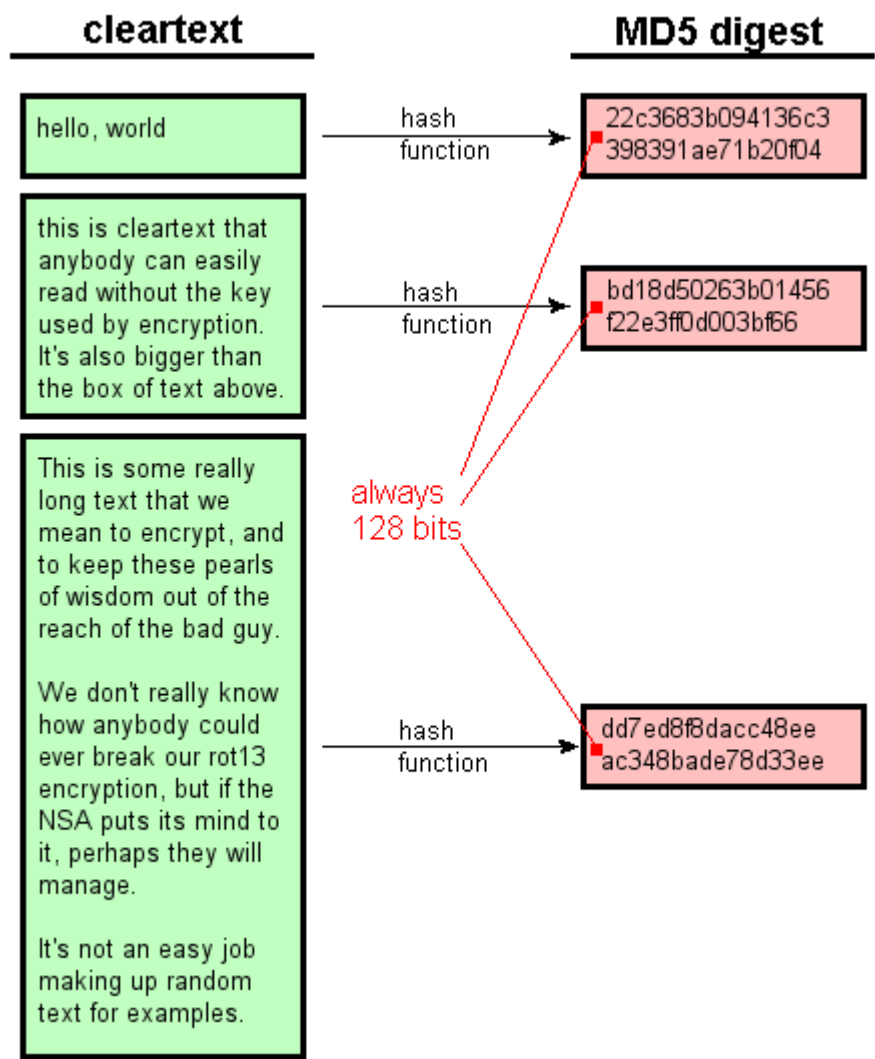


# PGP Decryption

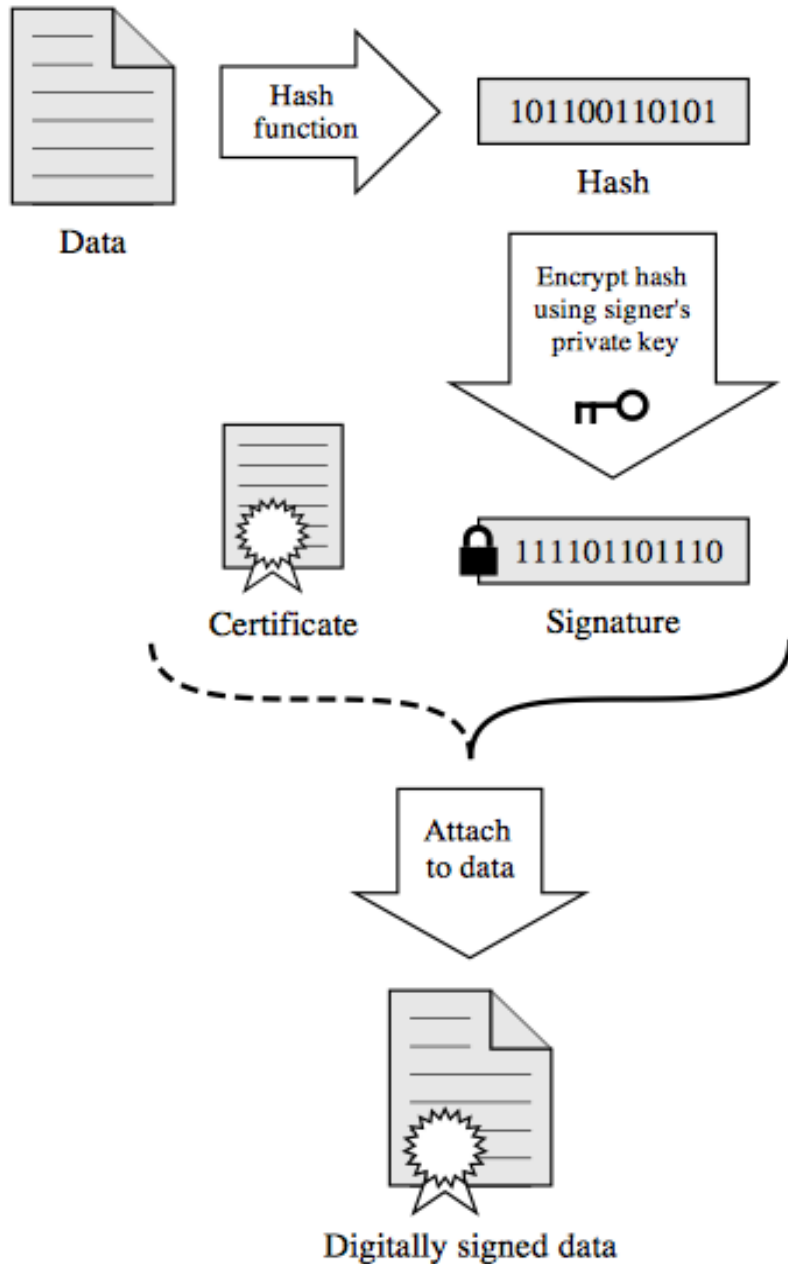


- Encryption offers
  - Confidentiality
  
- Digital Signatures offer
  - Authentication
  - Integrity

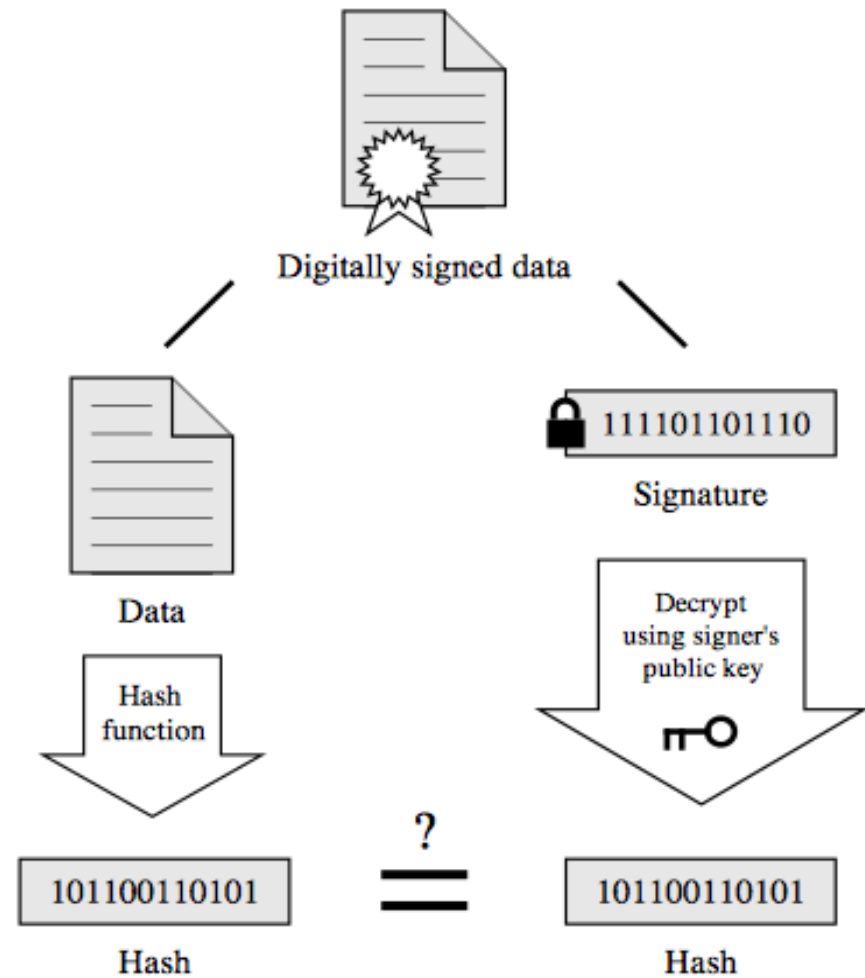




# Signing



# Verification

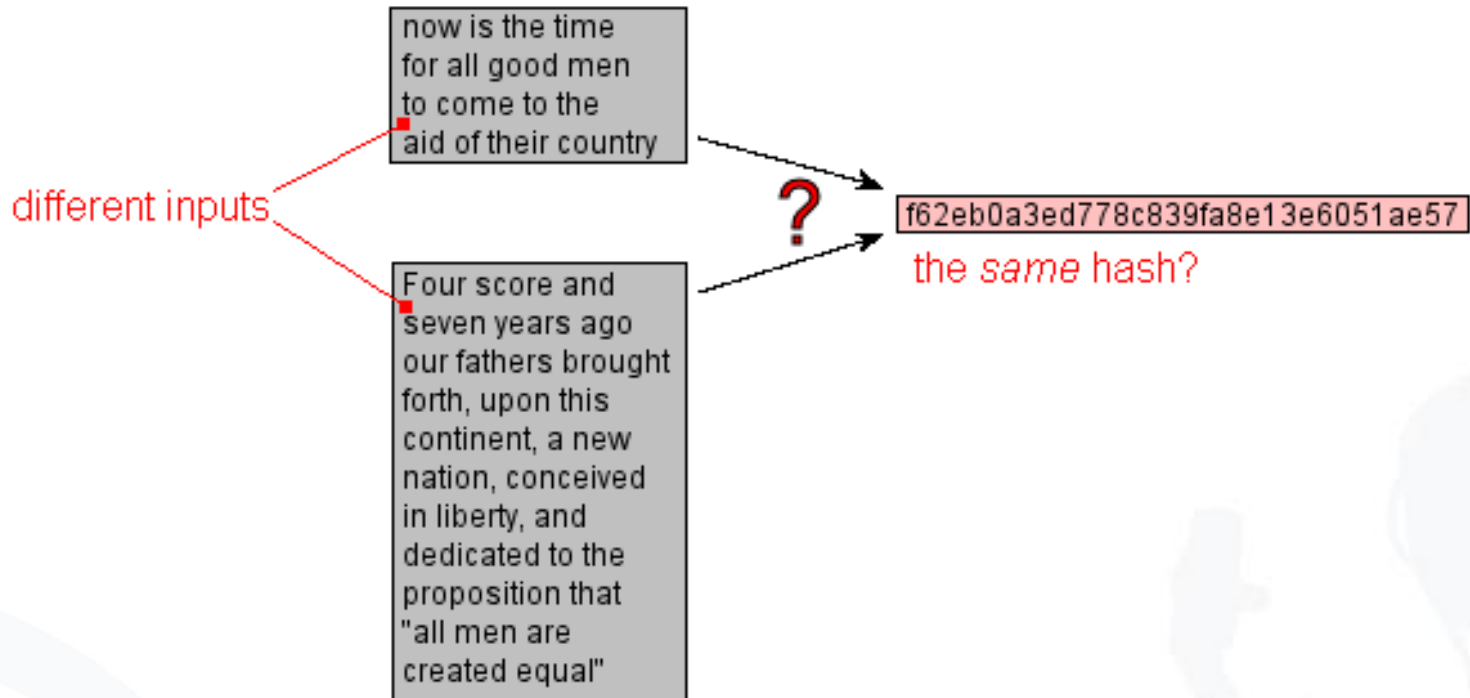


If the hashes are equal, the signature is valid.

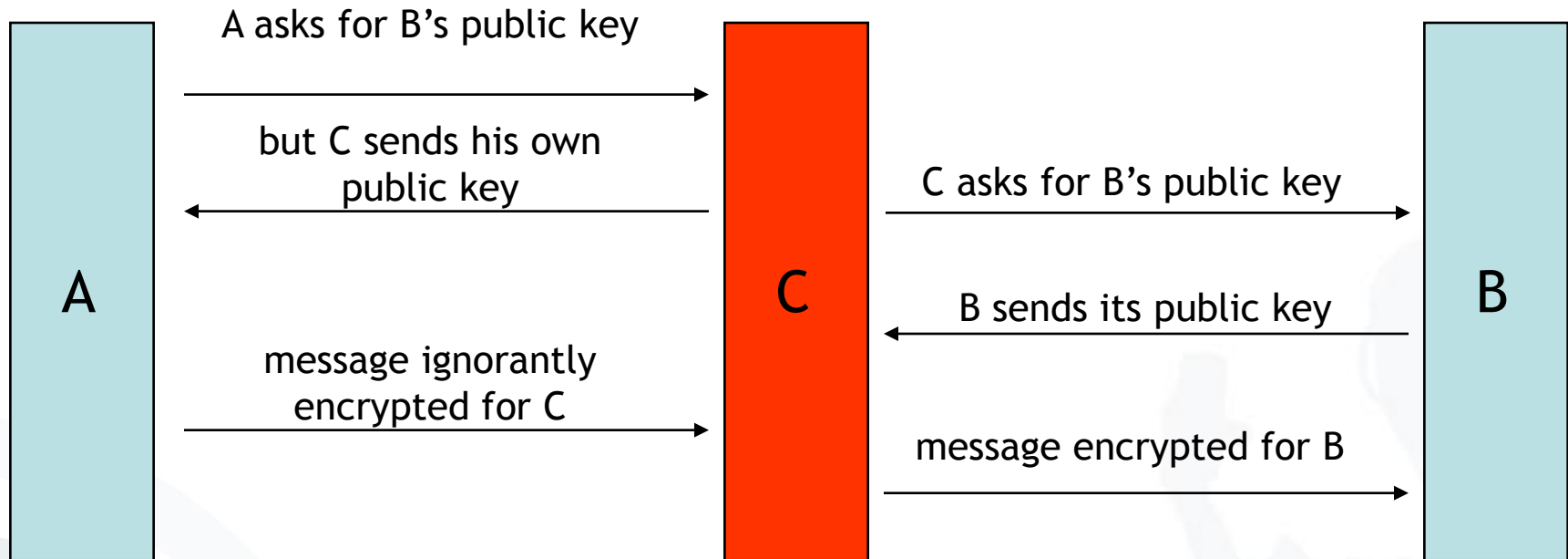
## Why Hash then Sign?

1. Efficiency: It's always faster to sign short messages (e.g. 160 bits) than large ones (MBs of a file).
2. Security: Someone can produce the signature of a message, without the secret key. E.g.:  $\text{sig}(M1 * M2) = \text{sig}(M1) * \text{sig}(M2)$

But then we need to make sure we don't have collisions  
 $\text{Sig}(\text{hash}(M1)) = \text{Sig}(\text{hash}(M2))$



## “Man in the middle attack”

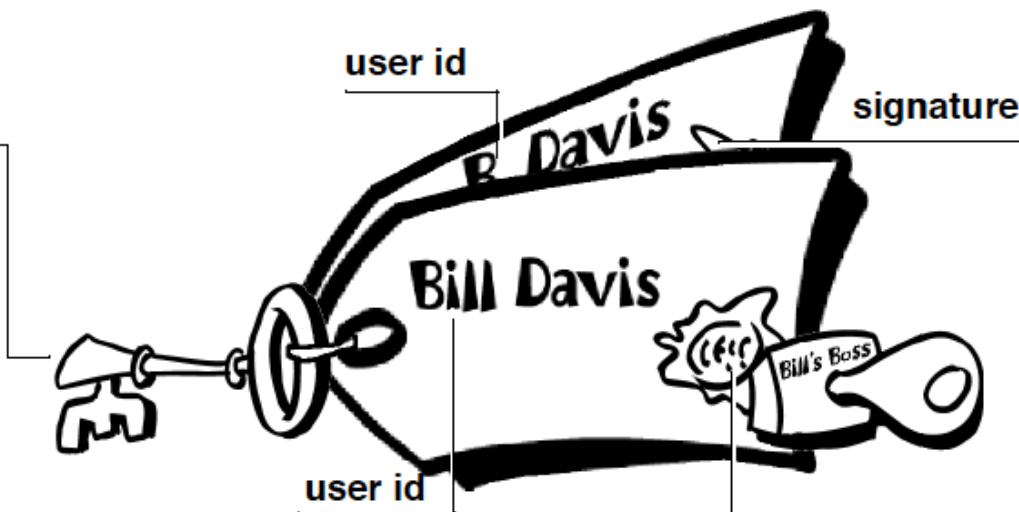


- ➔ Keys are certified, that means a third person/institution confirms (with its digital signature) the affiliation of the public key to a person

# PGP Digital Certificates

## public key

- PGP version number
- time when key created
- how long key is valid
- key type (DH, RSA)
- the key material itself



- string identifying the key's owner

## signature

- certification that the userid and key go together
- version number
- message digest algorithm
- message digest calculation
- signed message digest
- signer key id

# X.509 Digital Certificates

