Terms about Cryptography

GSE zExpertenforum April 2018

Peter Hunkeler
UBS Business Solutions AG

Cryptography – Cryptography? – Cryptography!

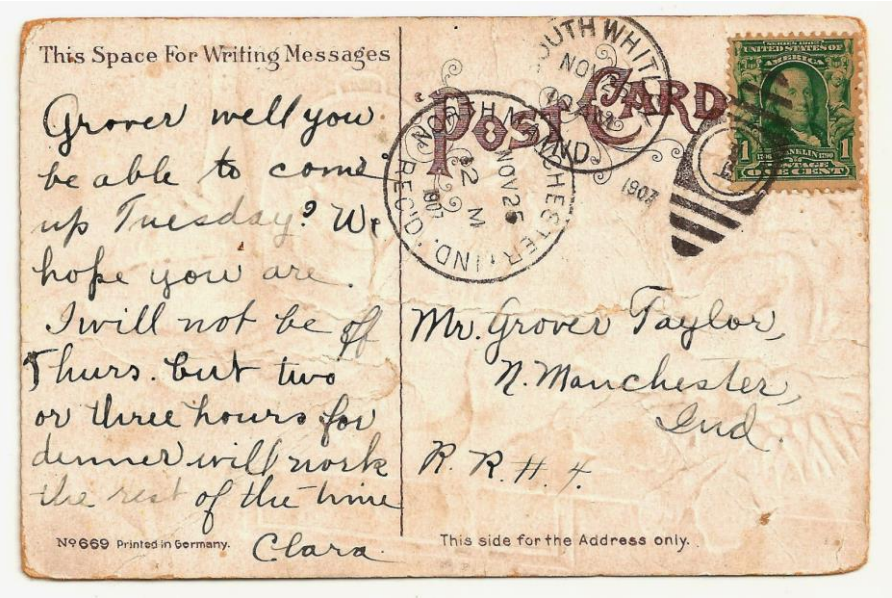
Encryption

Keys

Algorithms

Cryptography – Cryptography? – Cryptography!

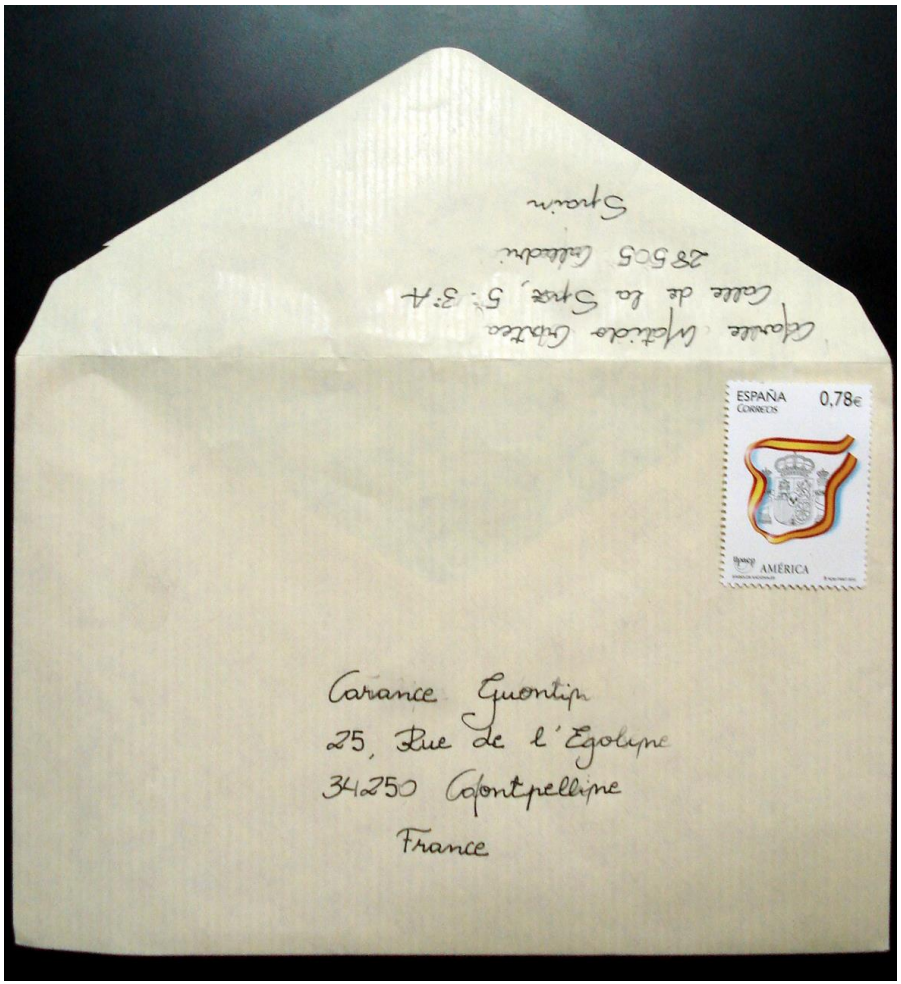
Post Cards – No Privacy



+ Low effort
+ Available everywhere

- Anyone can read the message
- Message cannot be verified
- Sender cannot be verified

First step to Privacy – Enveloped Mail



+ Message is protected.

Only a low force attack will unveil it.

- Message cannot be verified
- Sender cannot be verified

Identify Sender, Tamper-Proof – Sealed Envelope

+ Message is protected.

But a low force attack will still unveil it.

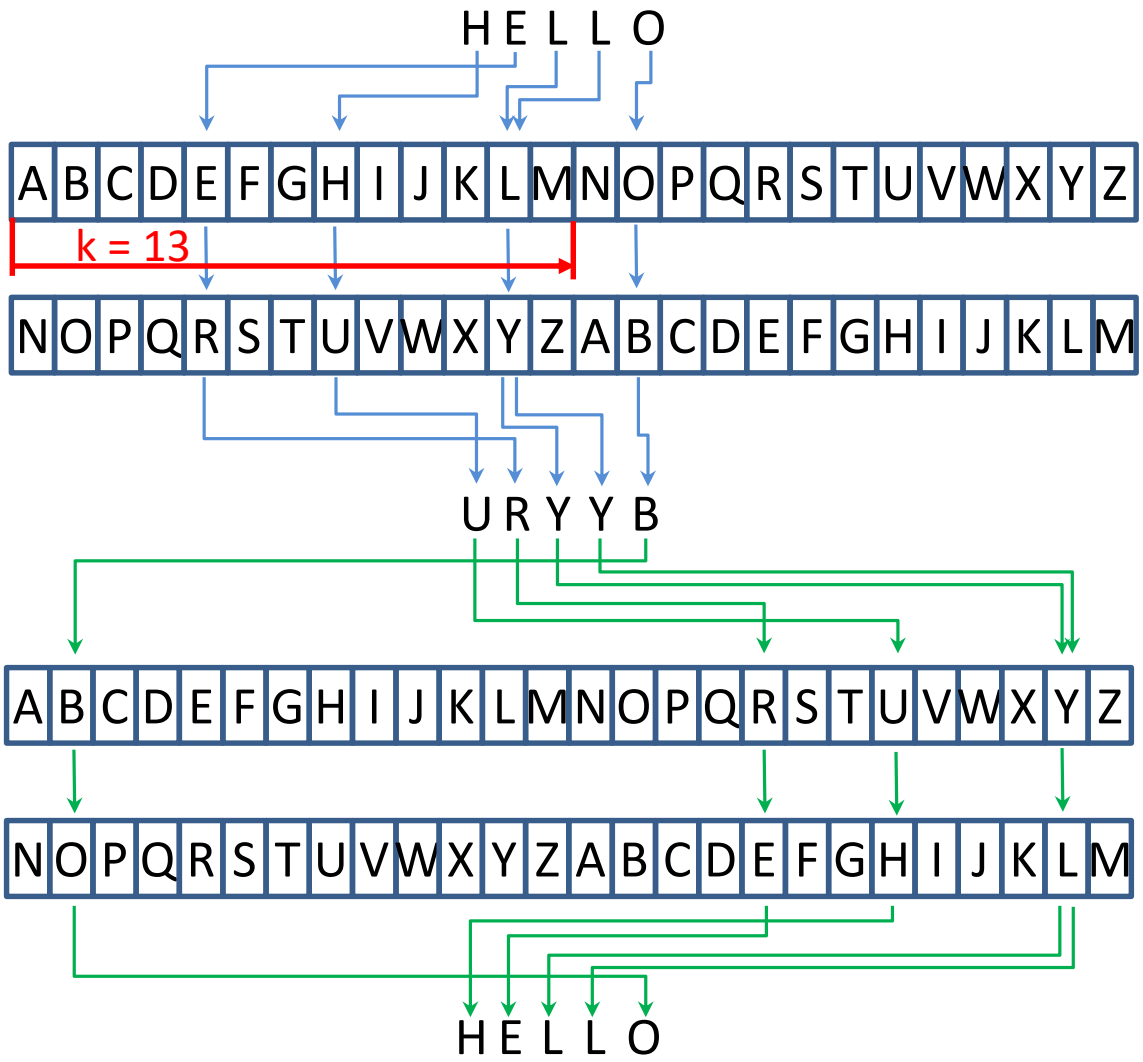
+ Message can be trusted

+ Sender can be verified

Store Data Safely – use a Safe – aka Encrypt Data

+ Message is strongly protected.
+ Message can be trusted.
+ Multiple users may know the key.
+ Brute force attach may succeed, but it takes high effort and long time.
- Key must be ***secretly*** communicated to receiver.
- Cannot verify sender if multiple user know the key.
- Key should be changed regularly.

Encryption Algorithm – aka Cipher

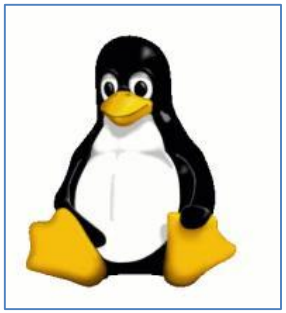


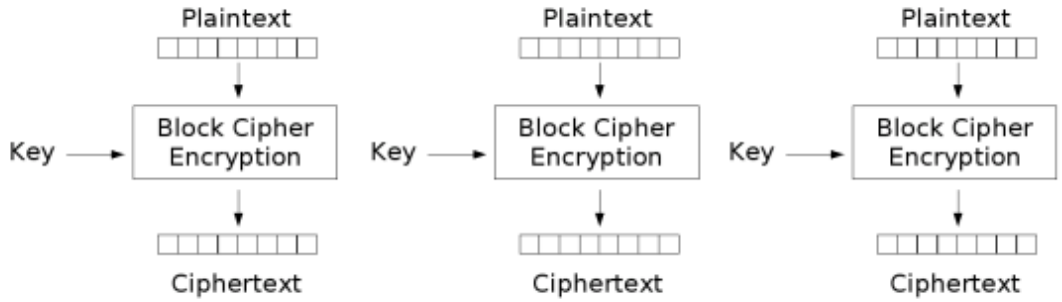
- ROT13 – a simple Algorithm
  - Rotate by k (key). k = 13
- Encryption algorithms transform information items.
  - Length preserved
- Algorithm called a *Cipher*
  - Stream ciphers → Byte by byte
  - Block ciphers → Blocks of bytes
- Mathematical formula to be applied
  - Parameter(s) influence result
- Parameters are
  - Key – a numeric value
  - Seed – a numeric value

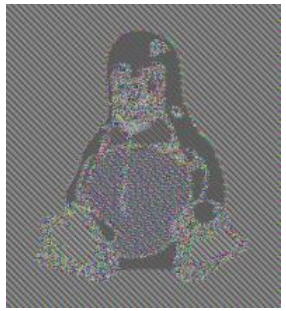
Symmetric Algorithms – Block Ciphers

Symmetric Algorithms – Stream Ciphers

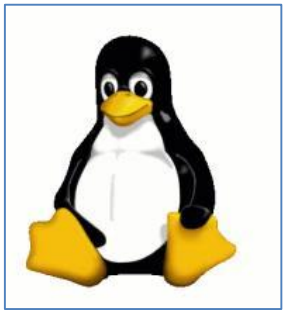
Block Cipher – Need to Chain Blocks Somehow

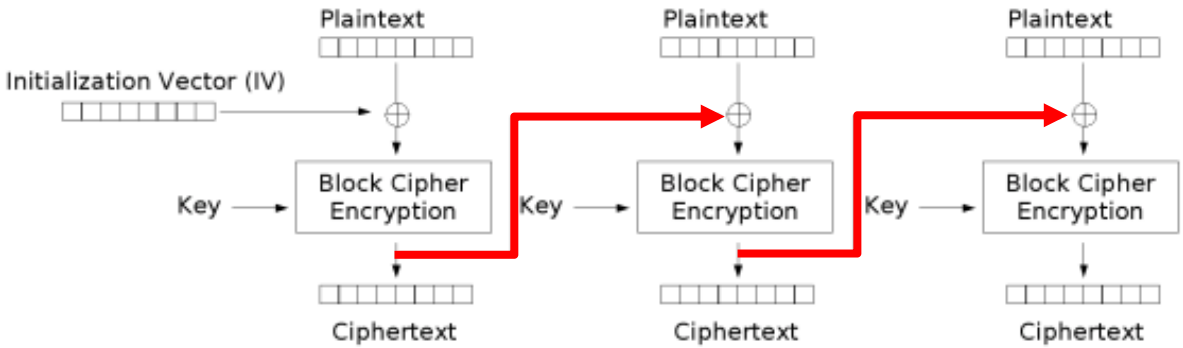


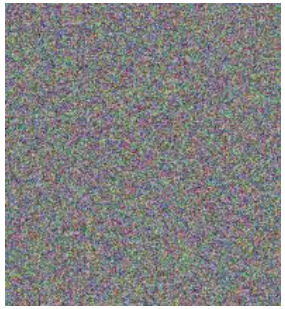




Electronic Codebook (ECB) mode encryption

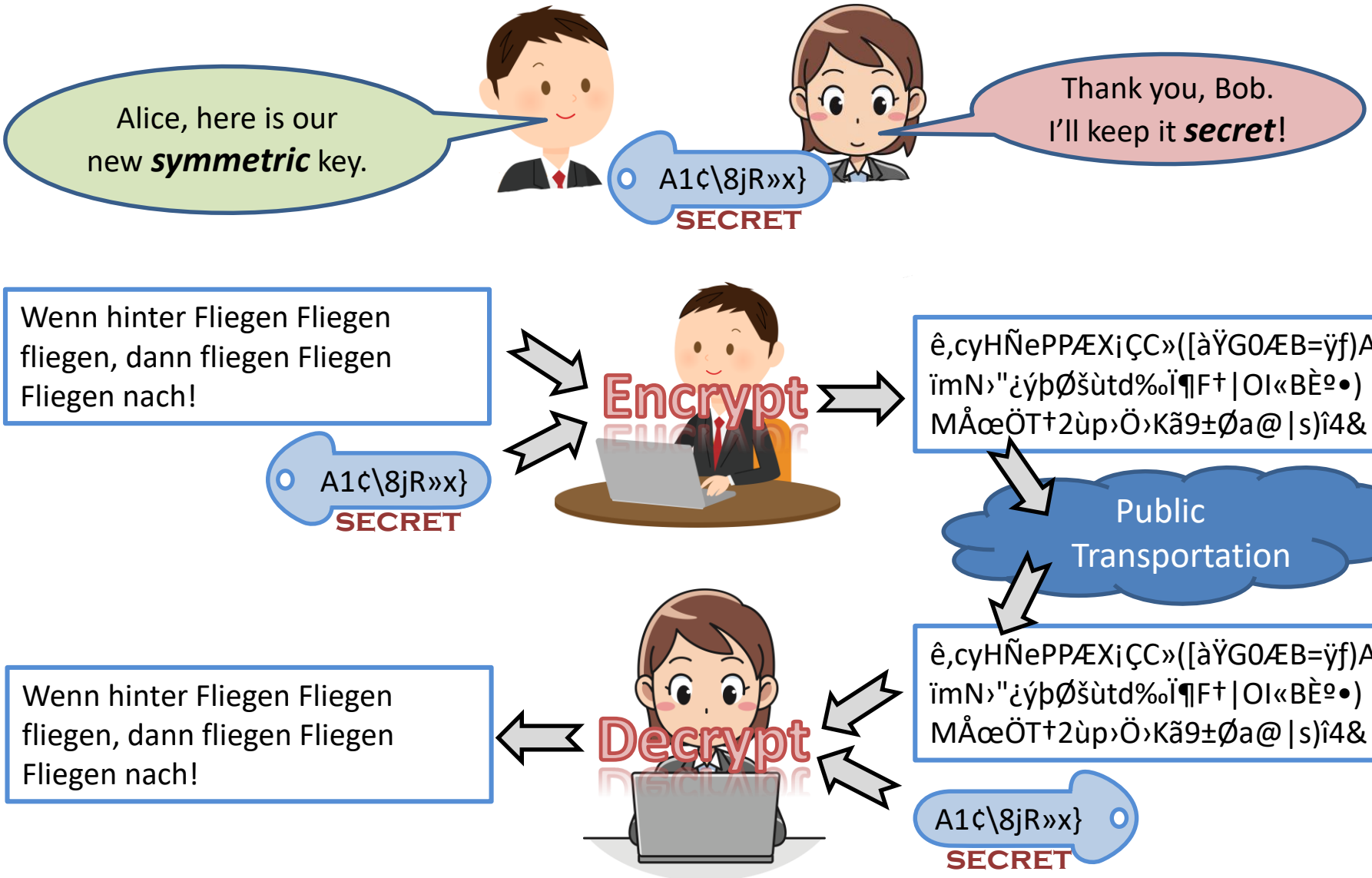






Cipher Block Chaining (CBC) mode encryption

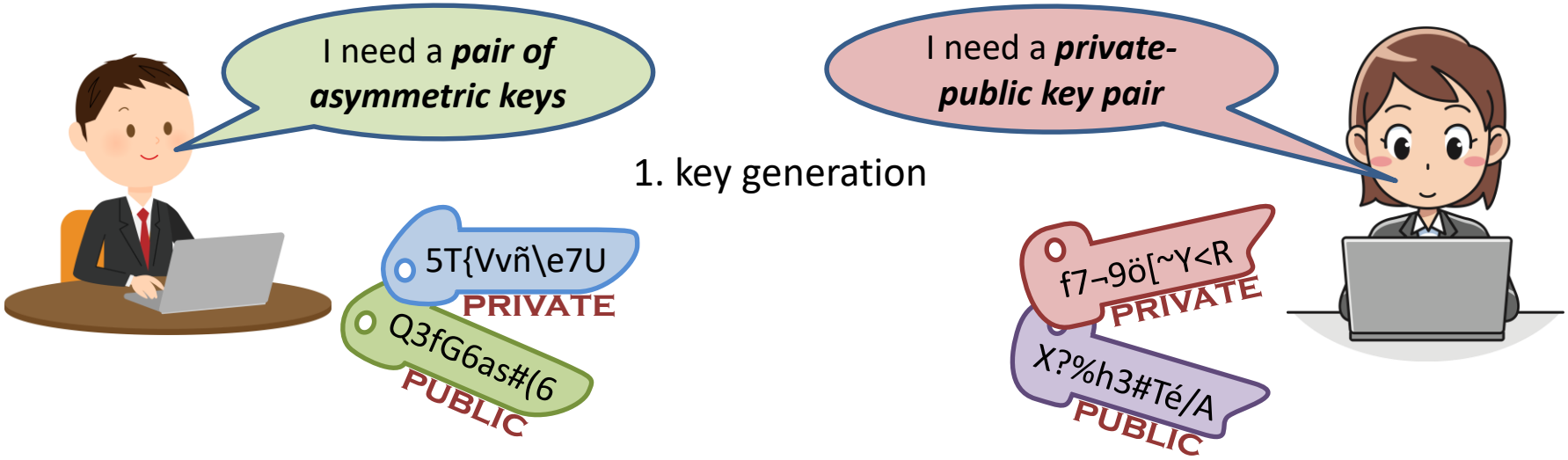
Symmetric Encryption – Secret Key Encryption



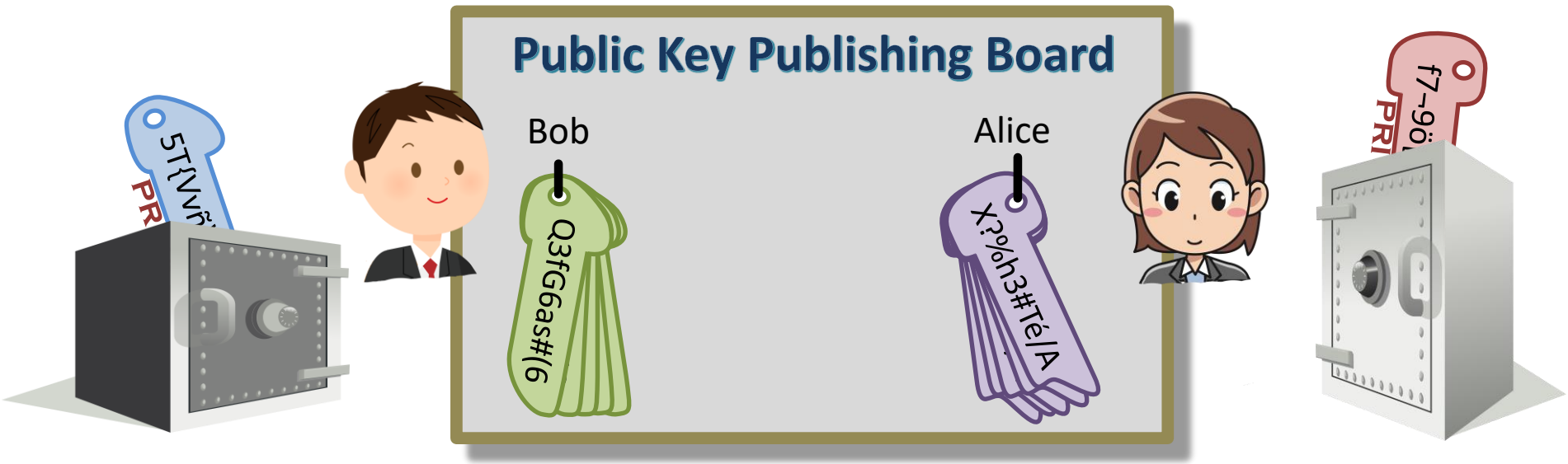
Asymmetric Algorithms – Asymmetric Ciphers

- RSA
- Diffie-Hellman Key Exchange Protocol
- ECC
- DSA

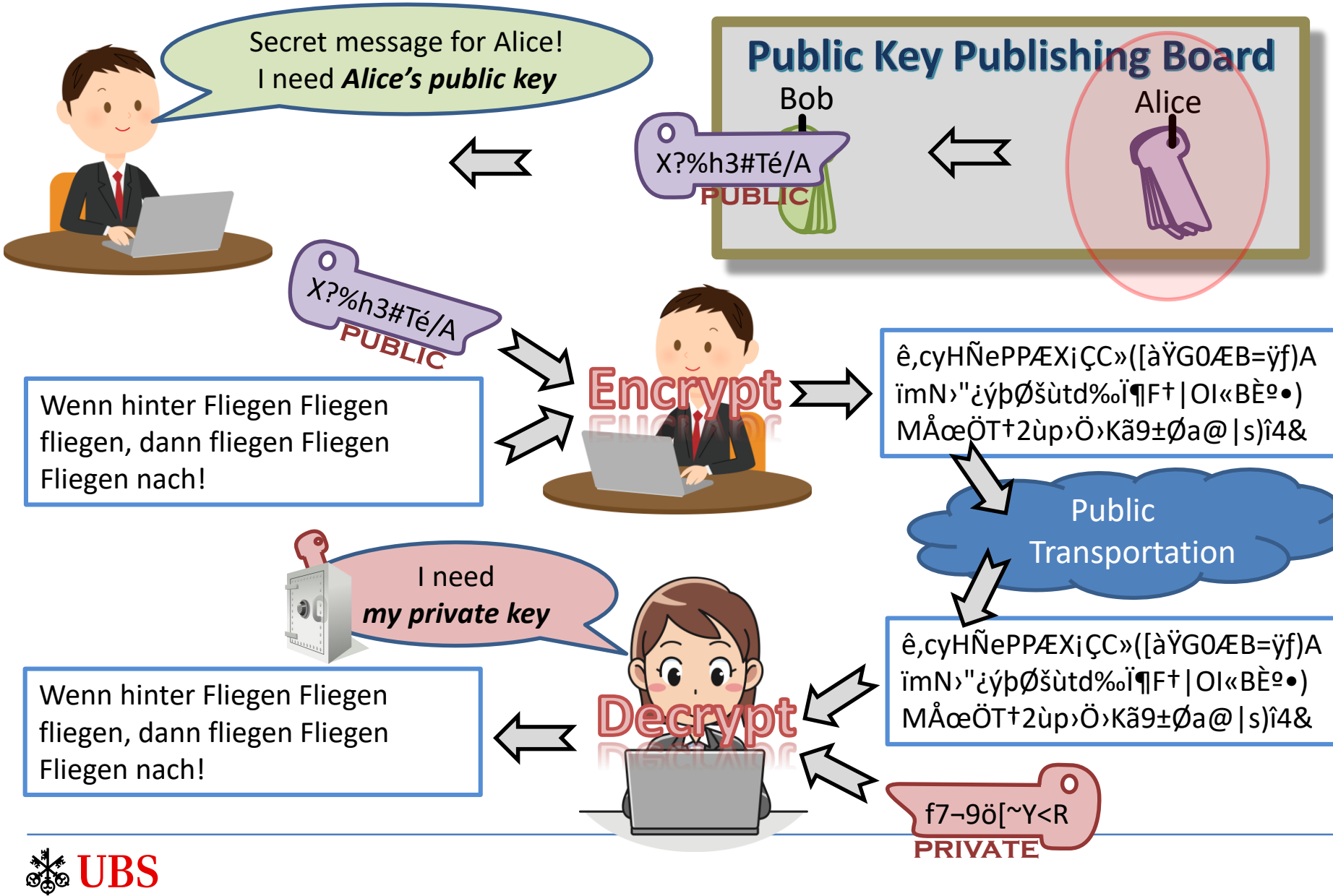
Asymmetric Encryption – Public Key Encryption



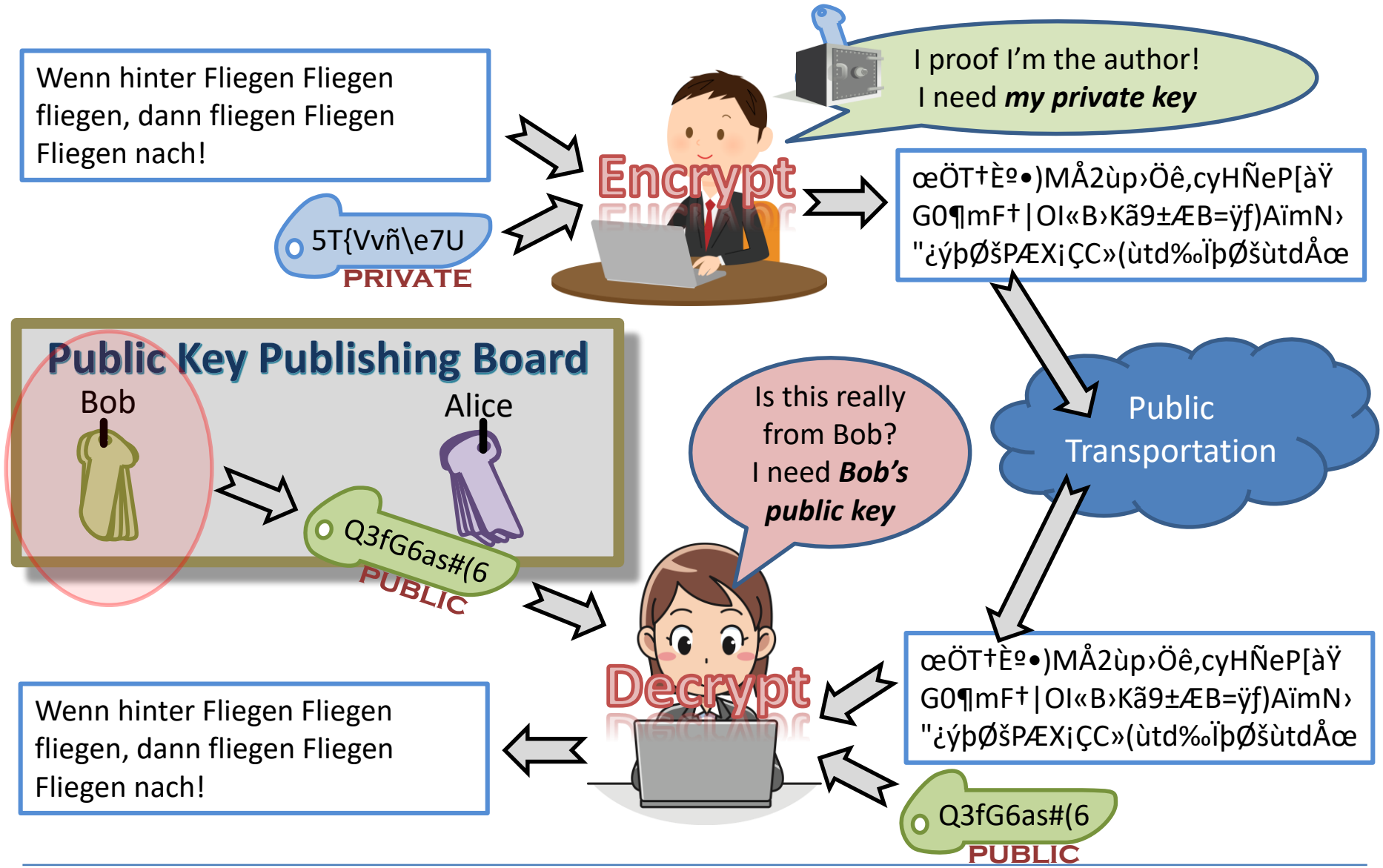
2. key distribution



Public Key Cryptography – Protect the Message



Public Key Cryptography– Identify Sender



Message Digest – Hash – Fingerprint

- SHA-0
- SHA-1
- SHA256
- SHA512
- HMAC
- MD2
- MD4
- MD5
- BLAKE2s, BLAKE2b
- HAVAL
- PANAMA
- Etc.

Message Digest – Hash – Fingerprint

Wenn hinter Fliegen Fliegen fliegen, dann fliegen Fliegen Fliegen nach!

x'716cc5203b913ea6e1029a696d538f3542c0b67d098645794b2040e3e83e739a'

Replace «!» by «.»

Wenn hinter Fliegen Fliegen fliegen, dann fliegen Fliegen Fliegen nach.

x'e8e7930cc48d03a85ed3dffc16aefb0197419e30433571bcc07872b47c4fdab5'

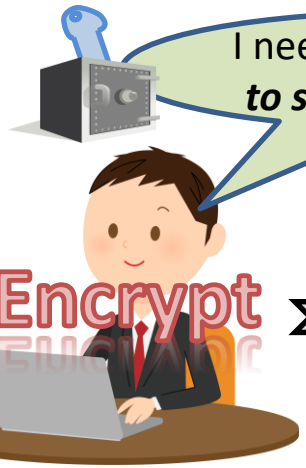
- Algorithm to create fixed-length value from variable-length data
- Create unique result:
  - Same input → same output
  - Tiny changes on input → completely different output
  - No two different input data result in same output (theoretically, at least)
  - No keys or other parameters involved
- One way
  - Cannot get back to input

Signing a Message – Integrity & Non-Repudiation

Wenn hinter Fliegen Fliegen fliegen,
dann fliegen Fliegen Fliegen nach!

x'716cc5203b913ea6e1029
a696d538f3542c0b67d0986
45794b2040e83e739a'

Message Digest



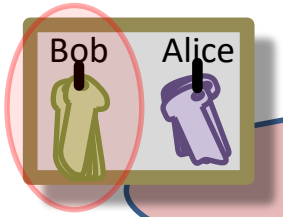
5T{Vvñ\e7U
PRIVATE

Signature

Ts†º•)2ù›Öê
,cÑàŸ¶mF†|
OI«B›KãBÿƒ)

Wenn hinter Fliegen Fliegen fliegen,
dann fliegen Fliegen Fliegen nach!

+



Is this really from Bob?
Is this what he really wrote?
I need ***Bob's public key***

Public Transportation

x'716cc5203b913ea6
e1029a696d538f3542
c0b67d098645794b2
040e3e83e739a'

Compare Equal?

Wenn hinter Fliegen Fliegen fliegen,
dann fliegen Fliegen Fliegen nach!

+

x'716cc5203b913ea6
e1029a696d538f3542
c0b67d098645794b2
040e3e83e739a'

Q3fG6as#(6
PUBLIC

+

Ts†º•)2ù›Öê
,cÑàŸ¶mF†|
OI«B›KãBÿƒ)

Digital Certificate – Creating a Digital Certificate

Hi, I need a certificate. Here is my data and my ***public key.***

Q3fG6as#(6

Bob's public

Certificate Information

Owner's Name:	Bob Topsecret
Owner's Public Key:	Q3fG6as#(6
Certificate Serial #:	4013401393012 2390782020948
Validity period:	2018-04-15 to 2020-04-14
Issuer's Name:	The Good CA
… (more)	…

Certificate Signature

2+f¬uÏDm{%w654?c3#`dg{>»së q¢=;dqpüfei9%a»\$§asd'añ£a2 wm:%ç0+f_re/!5<euä#%{\t^Ñs

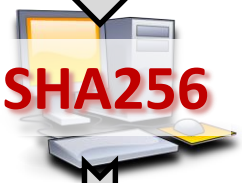
Bob's new Certificate

We verified this is Bob and it is his public key

The Good CA

Certificate Information

Owner's Name:	Bob Topsecret
Owner's Public Key:	Q3fG6as#(6
Certificate Serial #:	4013401393012 2390782020948
Validity period:	2018-04-15 to 2020-04-14
Issuer's Name:	The Good CA
… (more)	…



X?%h3#Té/A

The Good CA's private Key

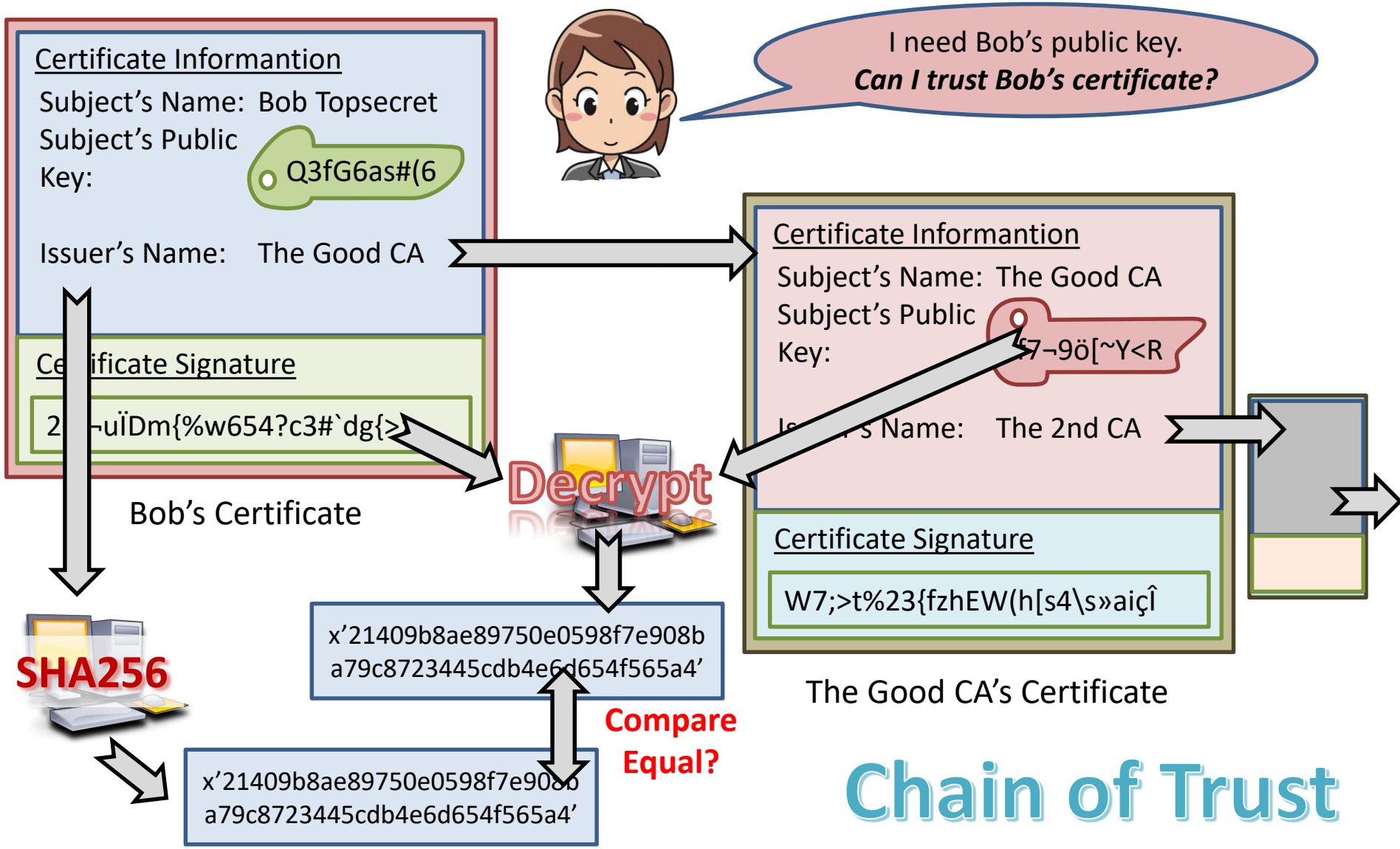
Encrypt

Certificate Signature

2+f¬uÏDm{%w654?c3#`dg{>»së q¢=;dqpüfei9%a»\$§asd'añ£a2 wm:%ç0+f_re/!5<euä#%{\t^Ñs

x'21409b8ae89750e0598f7e908b a79c8723445cdb4e6d654f565a4'

Digital Certificate – Verifying a Digital Certificate



Decryption with *raw Cipher* Succeeds with Any Key

Wenn hinter Fliegen Fliegen fliegen, dann fliegen Fliegen Fliegen nach!

A1¢\8jR»x}

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)A
ïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)
MÅœÖT†2ùp›Ö›Kã9±Øa@|s)î4&

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)A
ïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)
MÅœÖT†2ùp›Ö›Kã9±Øa@

Cq21é[+Va3

Heute scheint die Sonne; Vögel fangen hinter Fliegen fliegende Fliegen.

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)A
ïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)
MÅœÖT†2ùp›Ö›Kã9±Øa@

A1¢\8jR»x}

Wenn hinter Fliegen Fliegen fliegen, dann fliegen Fliegen Fliegen nach!

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)A
ïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)
MÅœÖT†2ùp›Ö›Kã9±Øa@

B#$3x/>1§a

Na# Du Kuchen Vög&6ä{e Fliegen das Zebra 33 krypti&alischer Mist hahaha

Encryption versus Compression

Wenn hinter Fliegen Fliegen fliegen, dann fliegen Fliegen Fliegen nach!

71 bytes

encrypt

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)AïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)MÅœÖT†2ùp›Ö›Kã9±Øa@|s)î4&

80 bytes

compress

CPWenn hinter F01 F01 f02, dann f01 F01 F01 nach!
CP01=liegenCP

47 + 9 + 6 = 62 bytes

compress, then encrypt

CPWenn hinter F01 F01 f02, dann f01 F01 F01 nach!
CP01=liegenCP

47 + 9 + 6 = 62 bytes

È¡FŠ³E5Â÷uùLÒèN"þ@y•Èç.Ô;ã/(îwƒZàfÓ,˜*8š!·v©;k‘jË¥p*g1I-\w½¿Ñ™‰Ï

64 bytes

encrypt, then compress

ê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)AïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)MÅœÖT†2ùp›Ö›Kã9±Øa@|s)î4&

80 bytes

CPê,cyHÑePPÆX¡ÇC»([àŸG0ÆB=ÿƒ)AïmN›"¿ýþØšùtd‰Ï¶F†|OI«BÈº•)MÅœÖT†2ùp›Ö›Kã9±Øa@|s)î4&
CPCP

80 + 6 = 86 bytes

UBS

Compression overhead

Questions