Securing Your E-Mail

— By using the GNU Privacy Guard —

Jan Tobias Mühlberg (KeyID 0x5BC905EC)
muehlber@fh-brandenburg.de

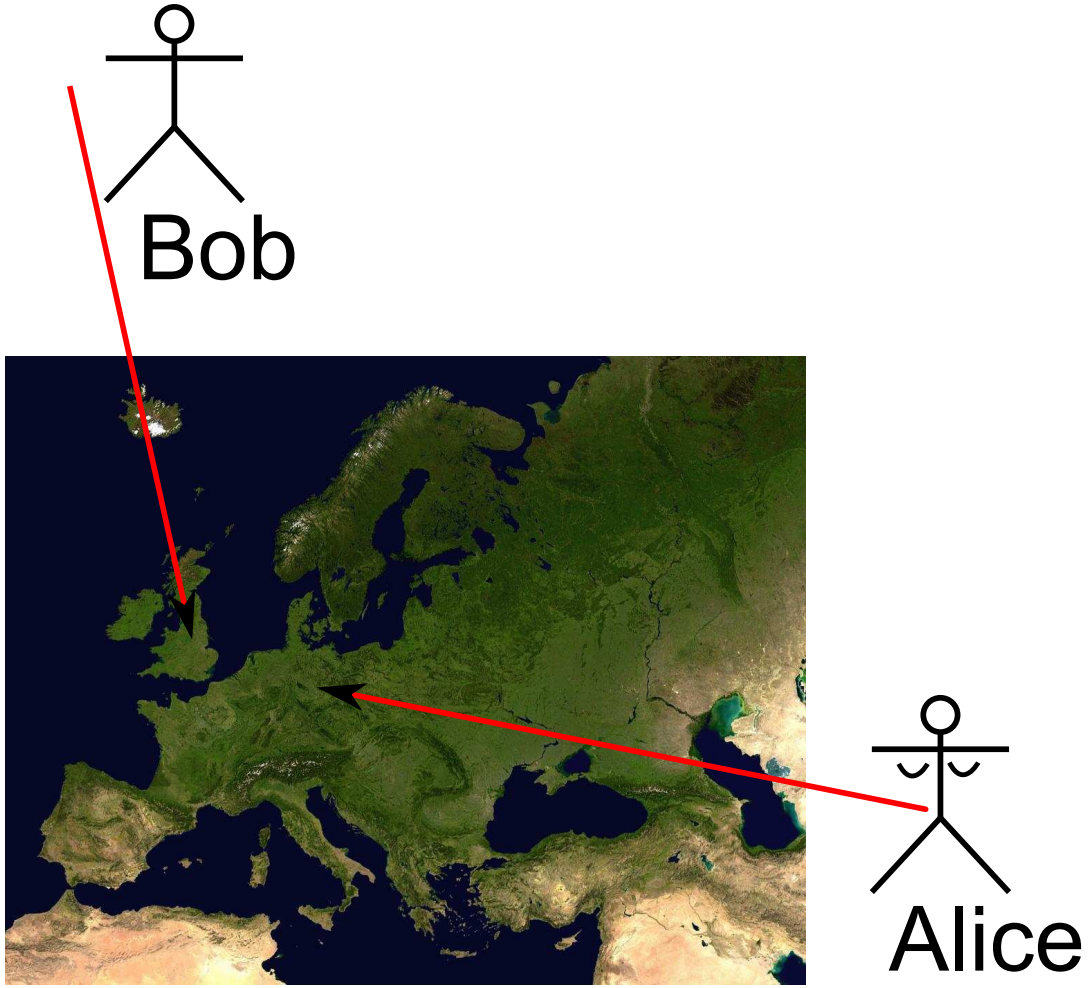
York Linux Users' Group

York, 17th October 2006

Outline

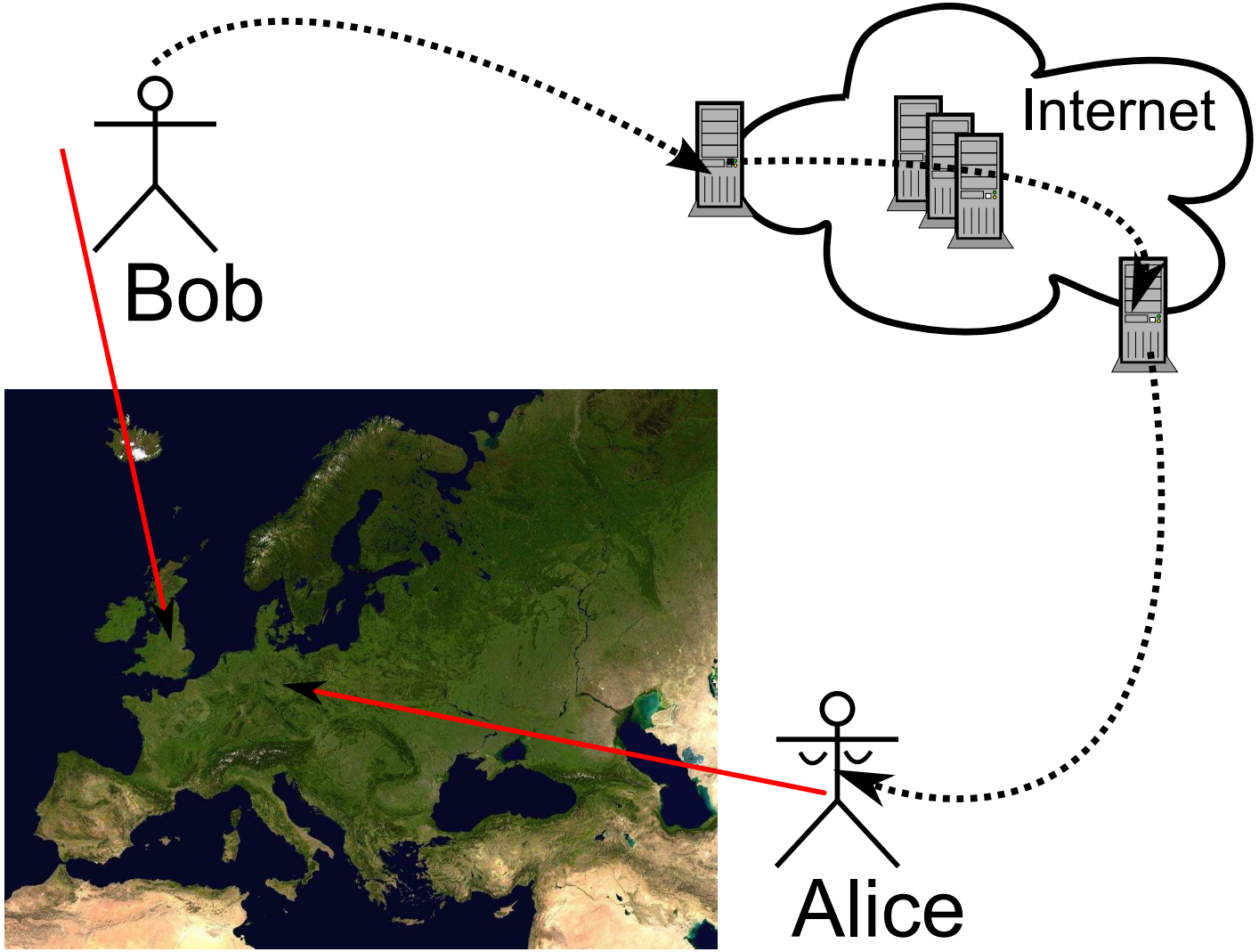
1. The story of Bob and Alice
2. A short intro to cryptography
3. The GNU Privacy Guard (GnuPG)
4. GnuPG Smart Cards
5. Well, is it secure?

The story of Bob and Alice



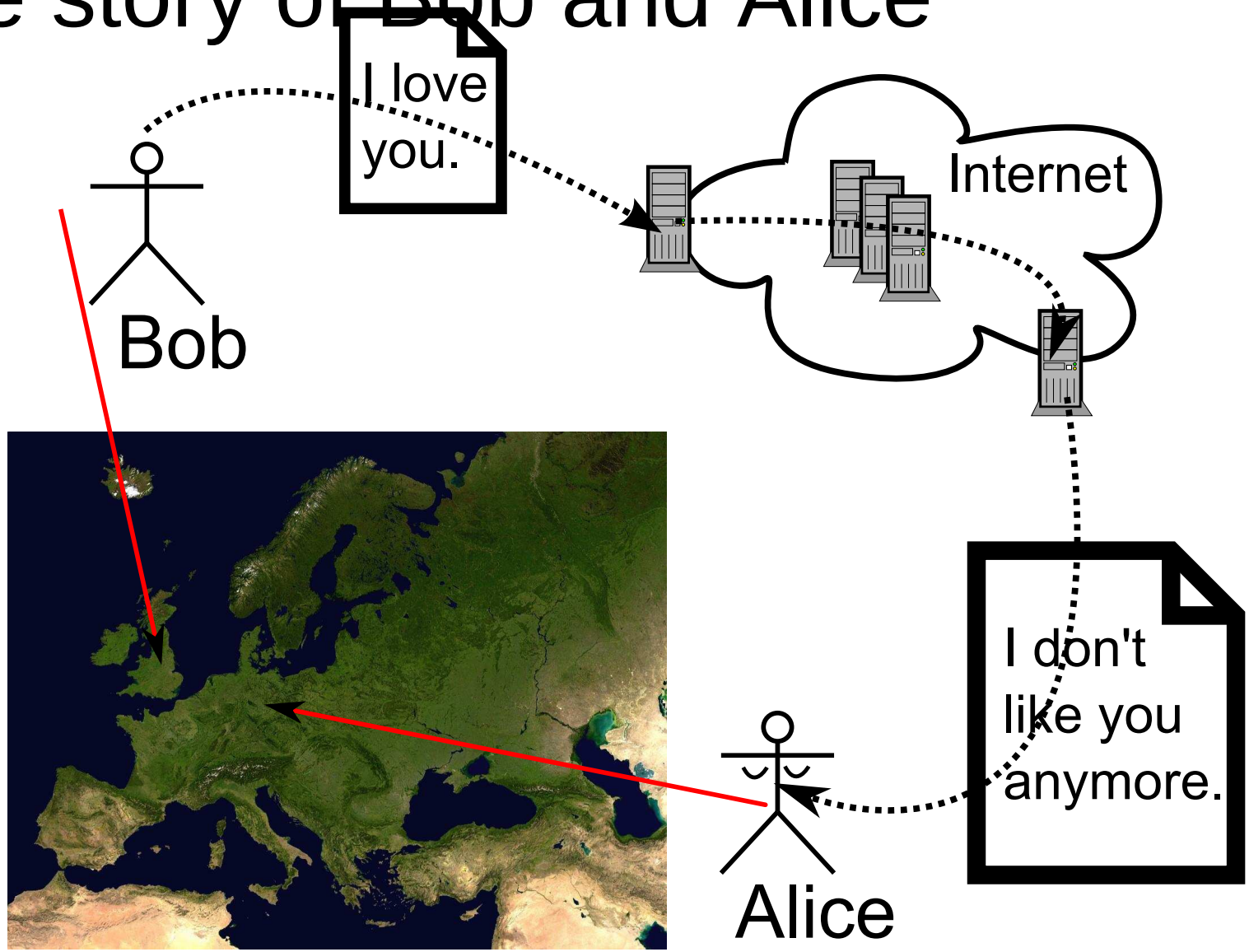
Picture of Europe taken from (NASA, 2002).

The story of Bob and Alice



Picture of Europe taken from (NASA, 2002).

The story of Bob and Alice



Picture of Europe taken from (NASA, 2002).

A short intro to cryptography

- It's all about **confidentiality**, **message integrity**, **authentication**, and **non-repudiation**.
- Terminology: We **encrypt** the **plaintext** of a message in order to convert it into something unintelligible known as the **ciphertext**. The ciphertext can be **decrypt**ed in order to get the plaintext back. A **cipher** is a pair of algorithms performing encryption and decryption. Most ciphers require a **key**.

A short intro to cryptography

- It's all about **confidentiality**, **message integrity**, **authentication**, and **non-repudiation**.
- Terminology: We **encrypt** the **plaintext** of a message in order to convert it into something unintelligible known as the **ciphertext**. The ciphertext can be **decrypt**ed in order to get the plaintext back. A **cipher** is a pair of algorithms performing encryption and decryption. Most ciphers require a **key**.

Symmetric-Key Ciphers

- Caesar-Cipher:

plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m
ciphertext:	D	E	F	G	H	I	J	K	L	M	N	O	P
plaintext:	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- An example:

LORYHBRX ≈ iloveyou

- **Symmetric-key** ciphers use the same key for encryption and decryption.

Symmetric-Key Ciphers

- Caesar-Cipher:

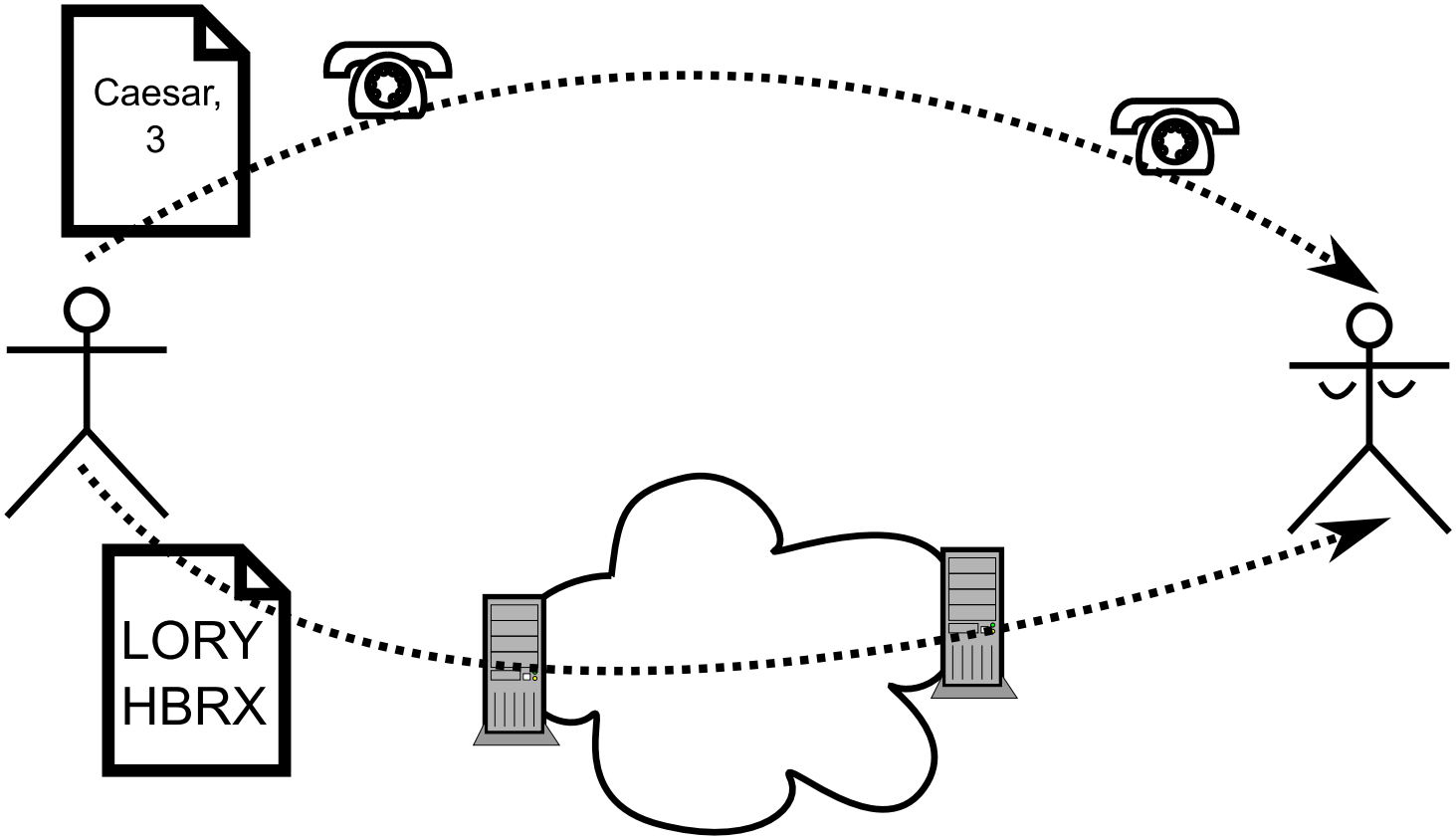
plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m
ciphertext:	D	E	F	G	H	I	J	K	L	M	N	O	P
plaintext:	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- An example:

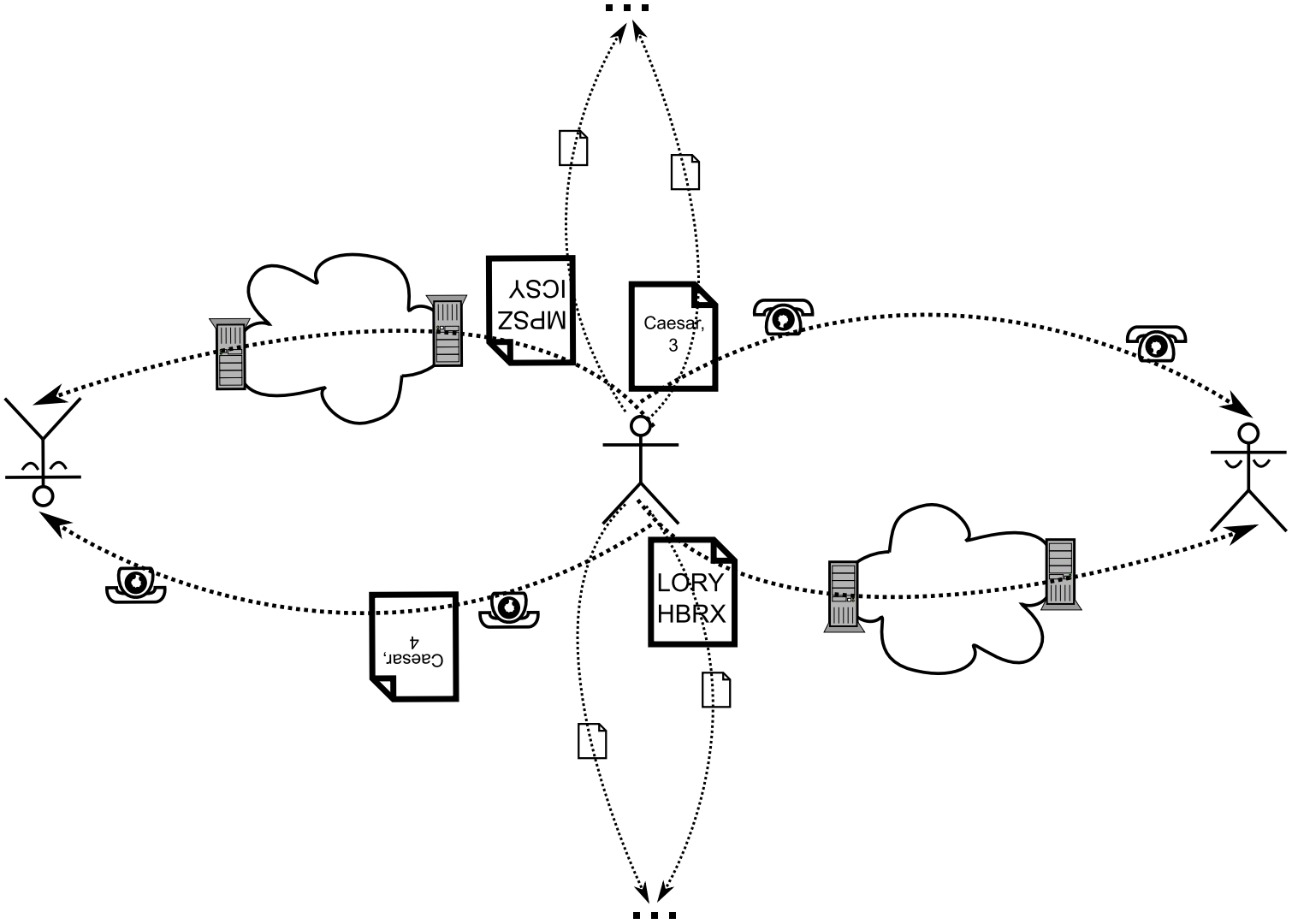
LORYHBRX ≈ iloveyou

- **Symmetric-key** ciphers use the same key for encryption and decryption.

Symmetric-Key Ciphers



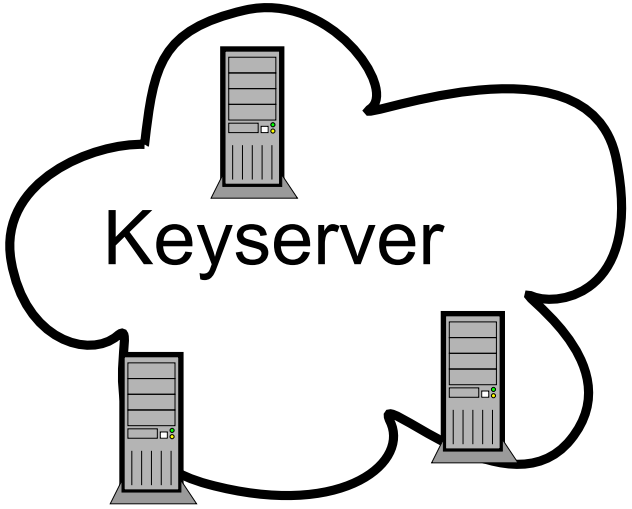
Symmetric-Key Ciphers

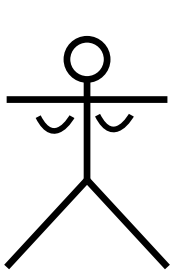


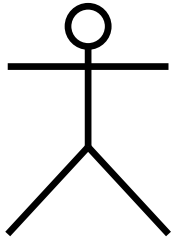
Asymmetric-Key Ciphers

- **Asymmetric-key** ciphers (also: public-key ciphers) use a pair of keys for each party.
- The **private key** and the **public key** are both generated in secret. **Only the private key is kept secret**.
- A message **encrypted with a party's public key** can be **decrypted with the related private key**; vice versa.

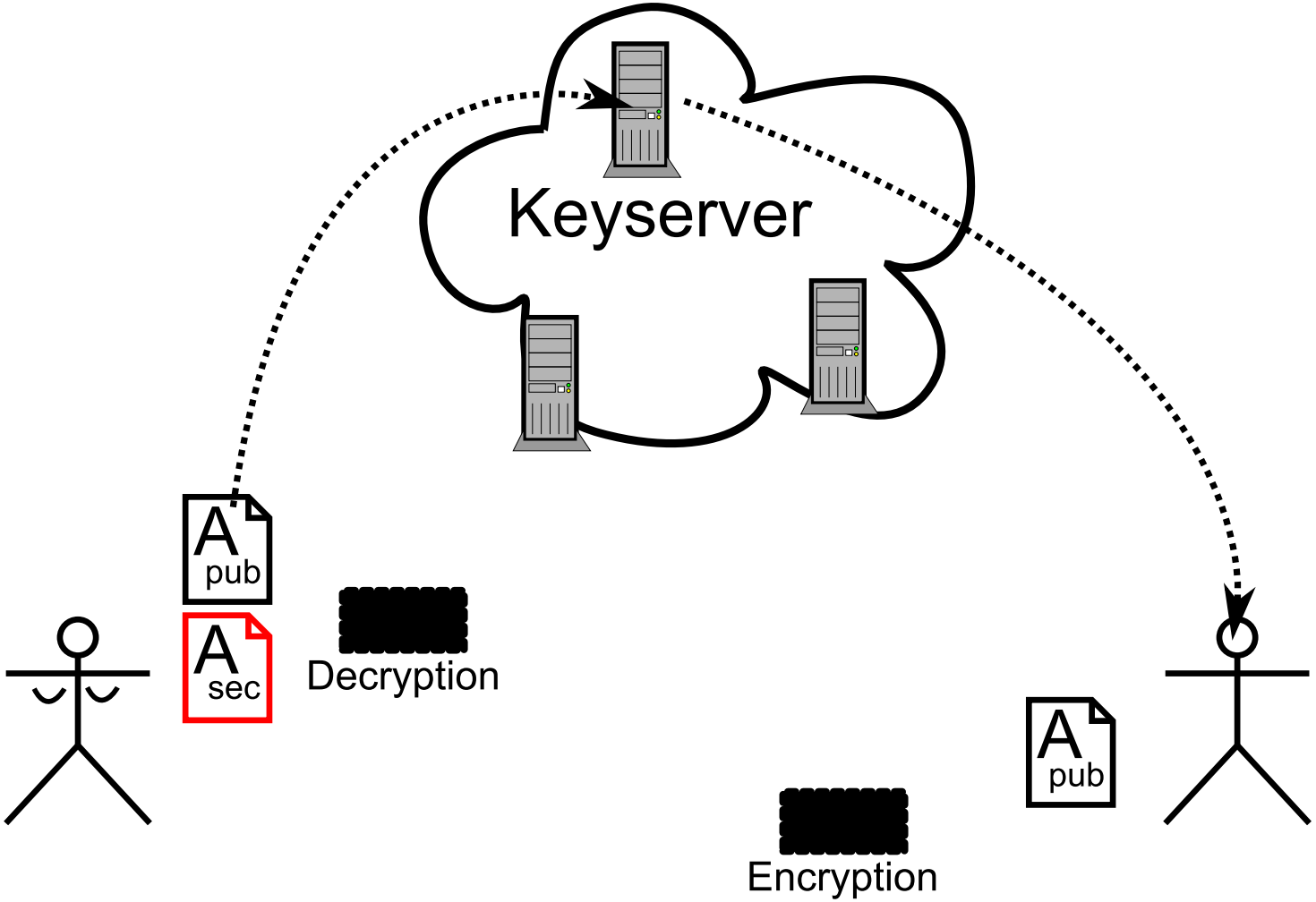
Encryption and Decryption



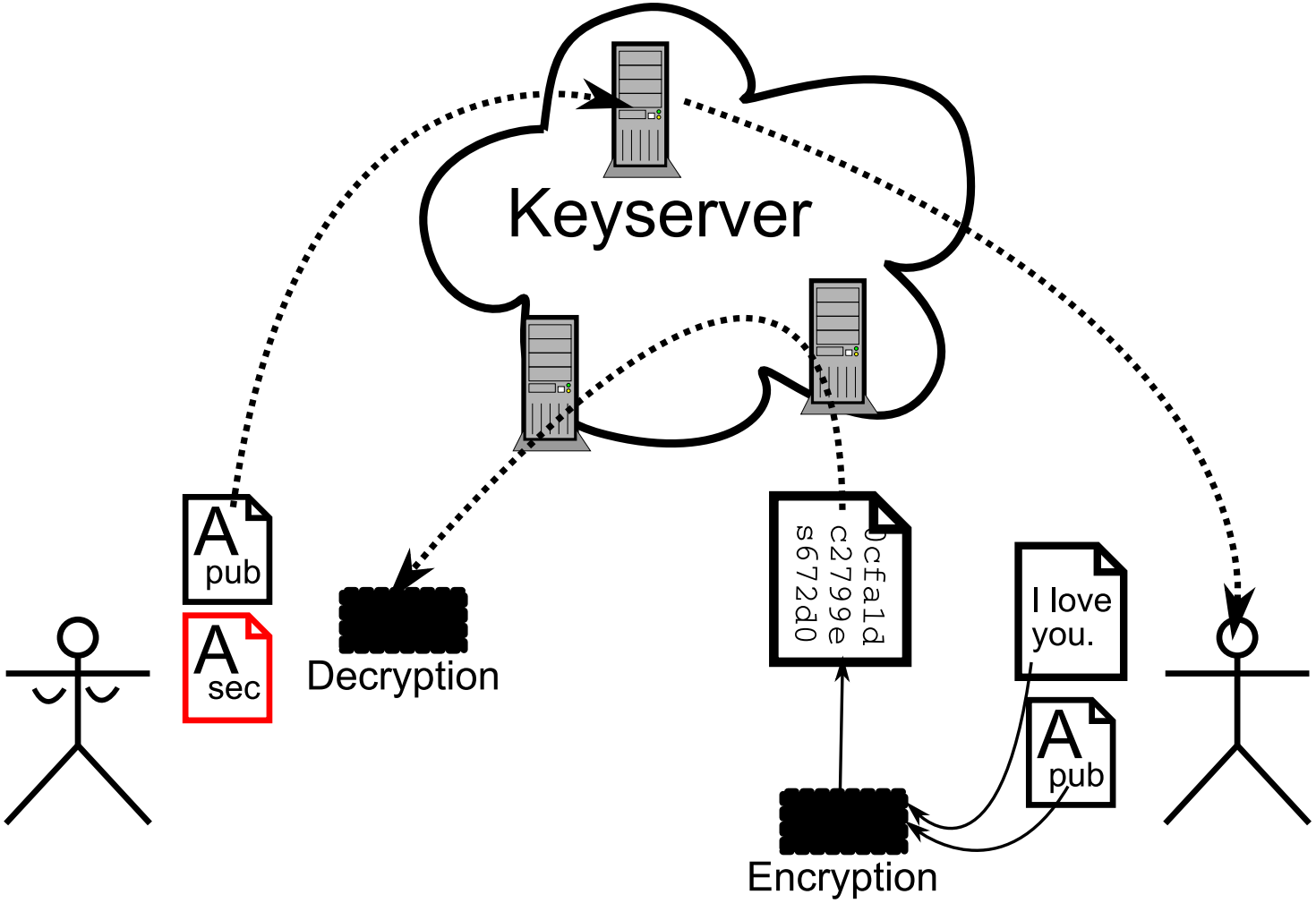




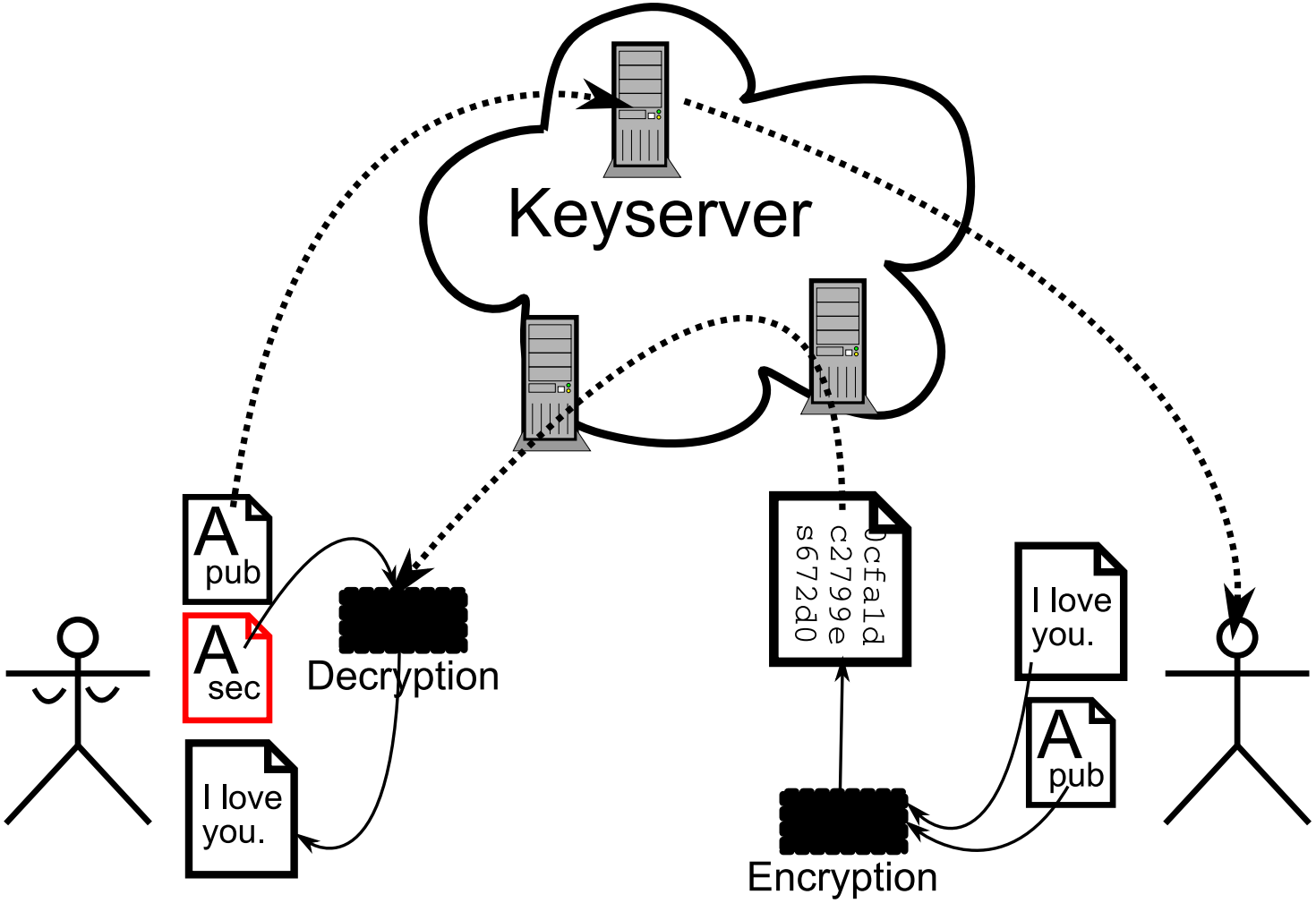
Encryption and Decryption



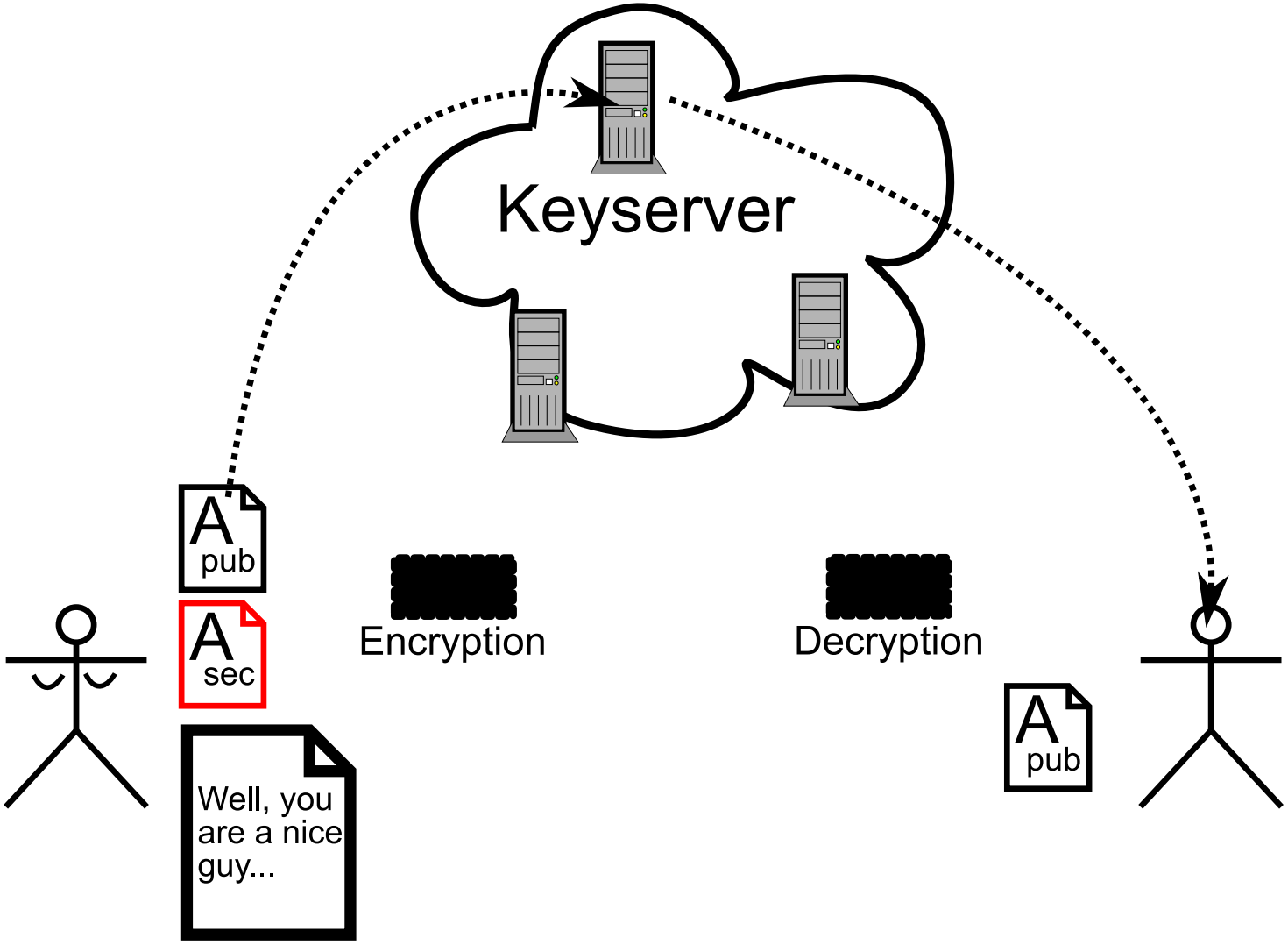
Encryption and Decryption



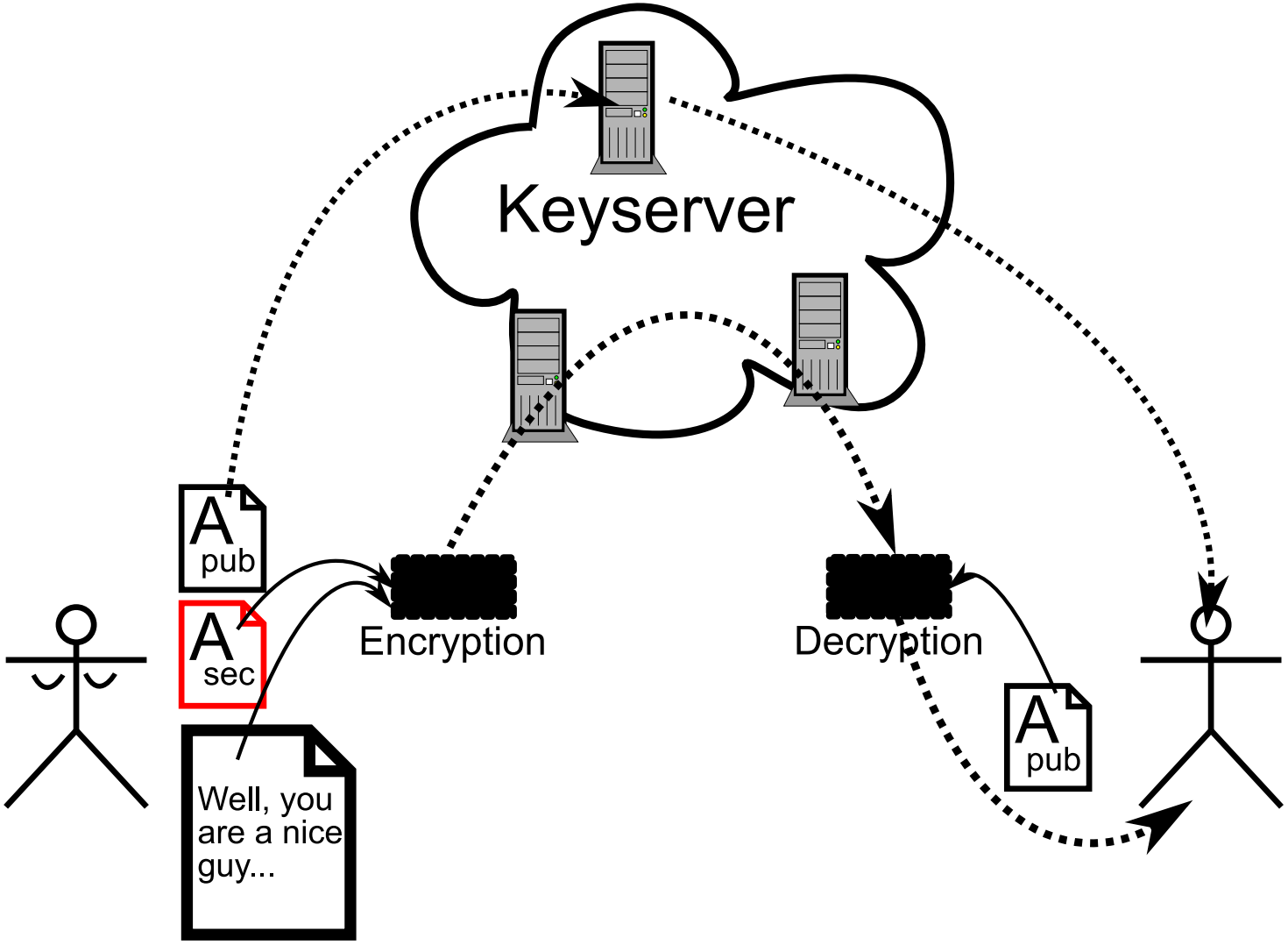
Encryption and Decryption



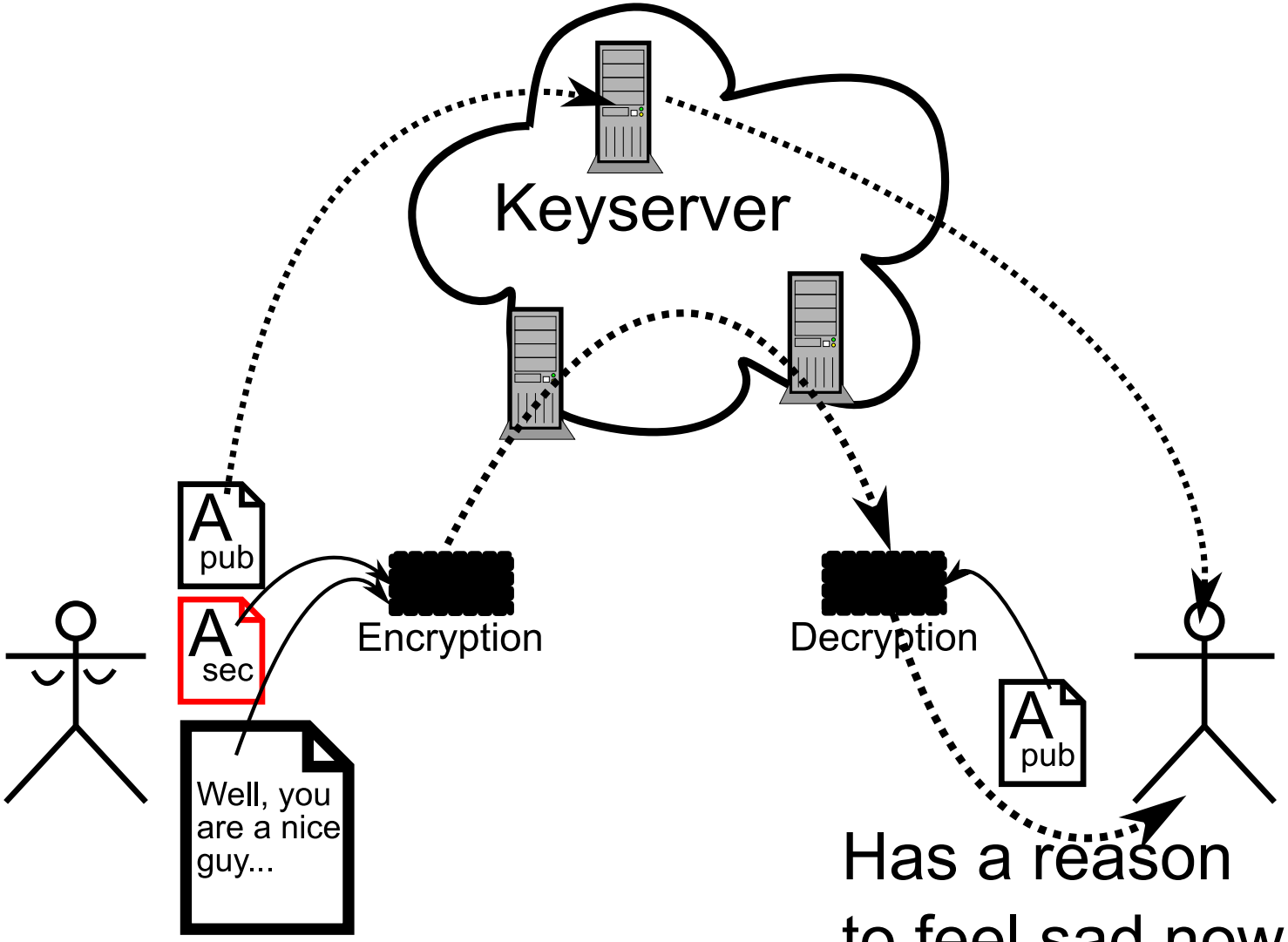
Generating Signatures



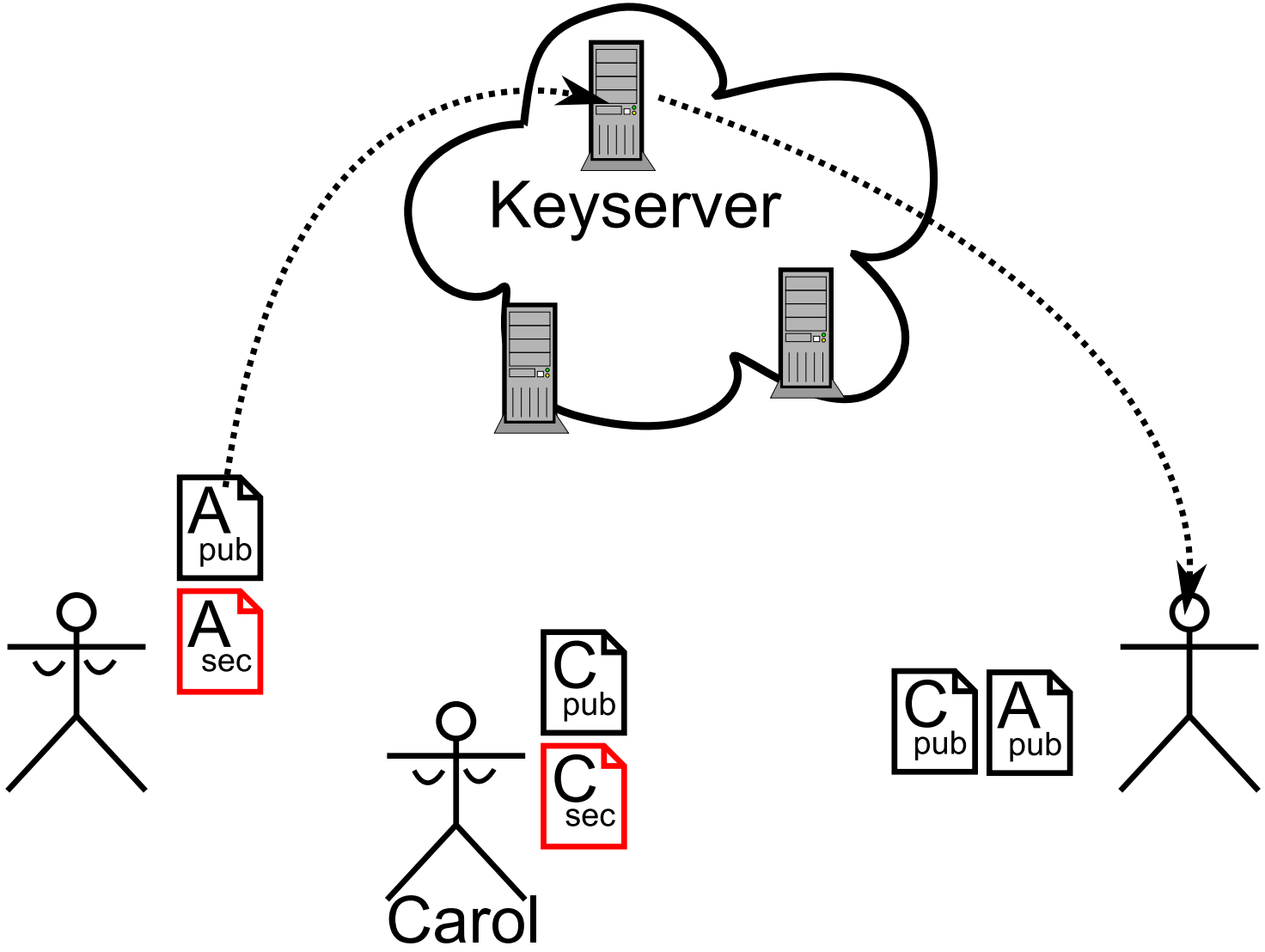
Generating Signatures



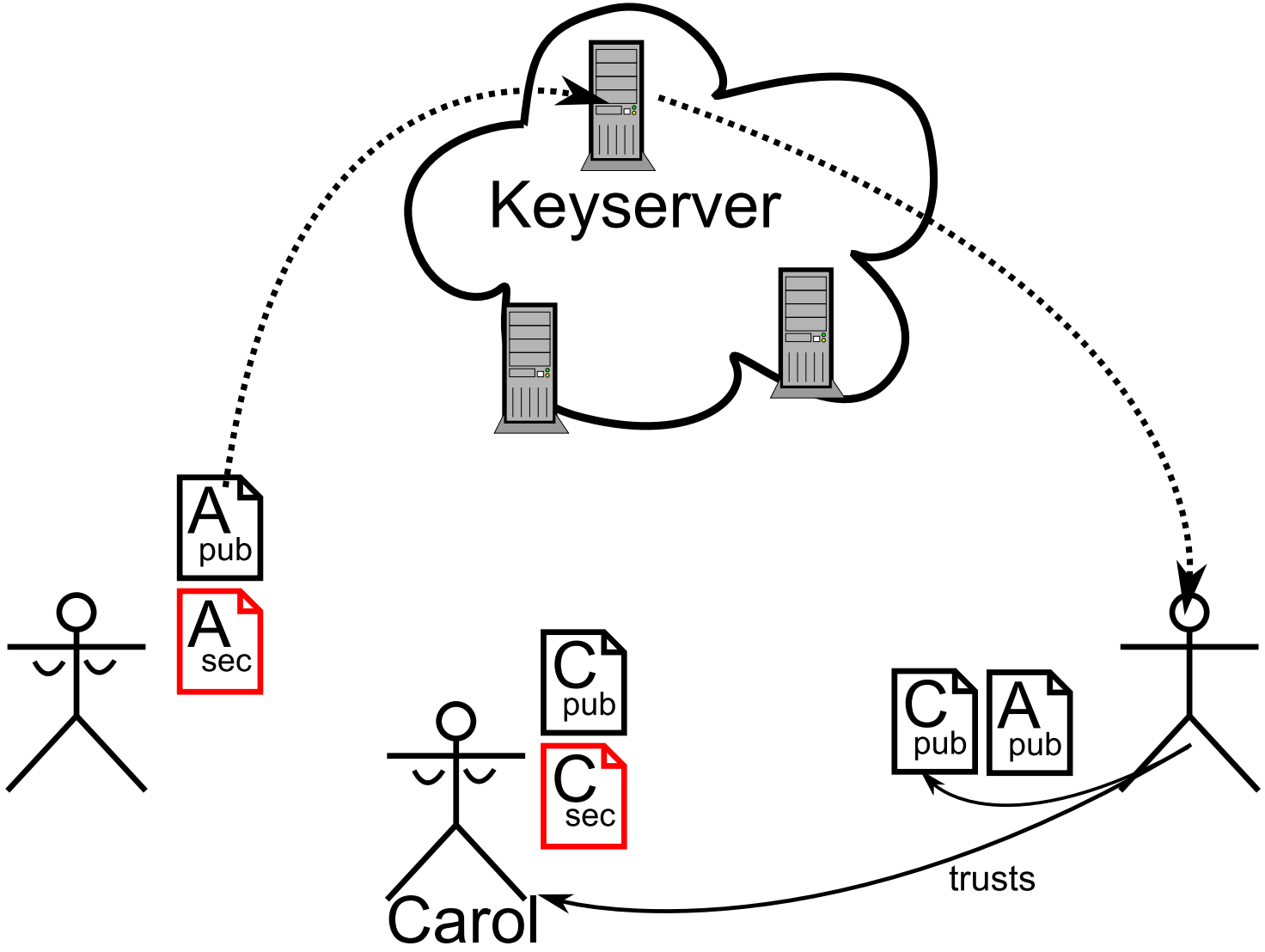
Generating Signatures



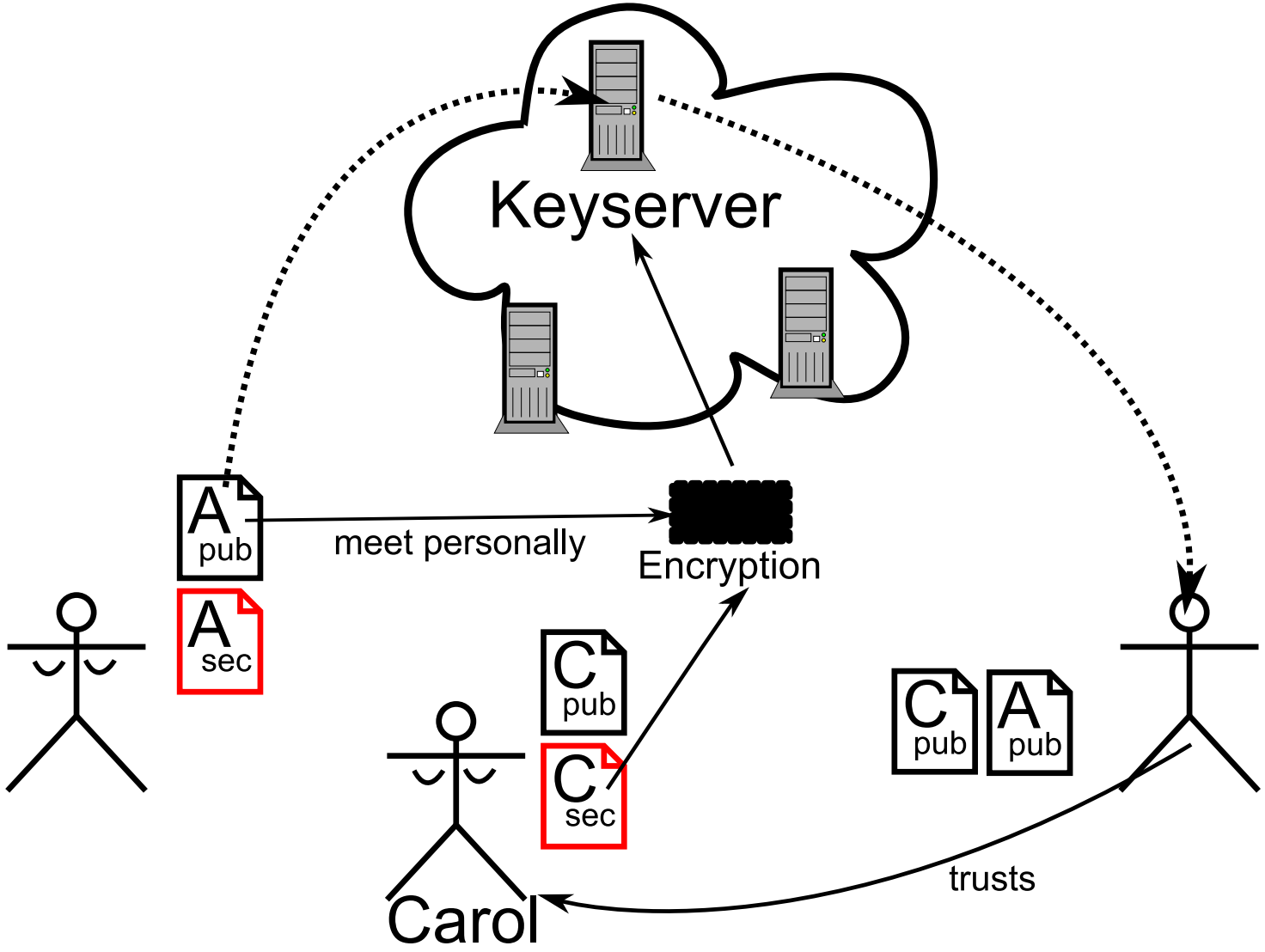
Key Signing



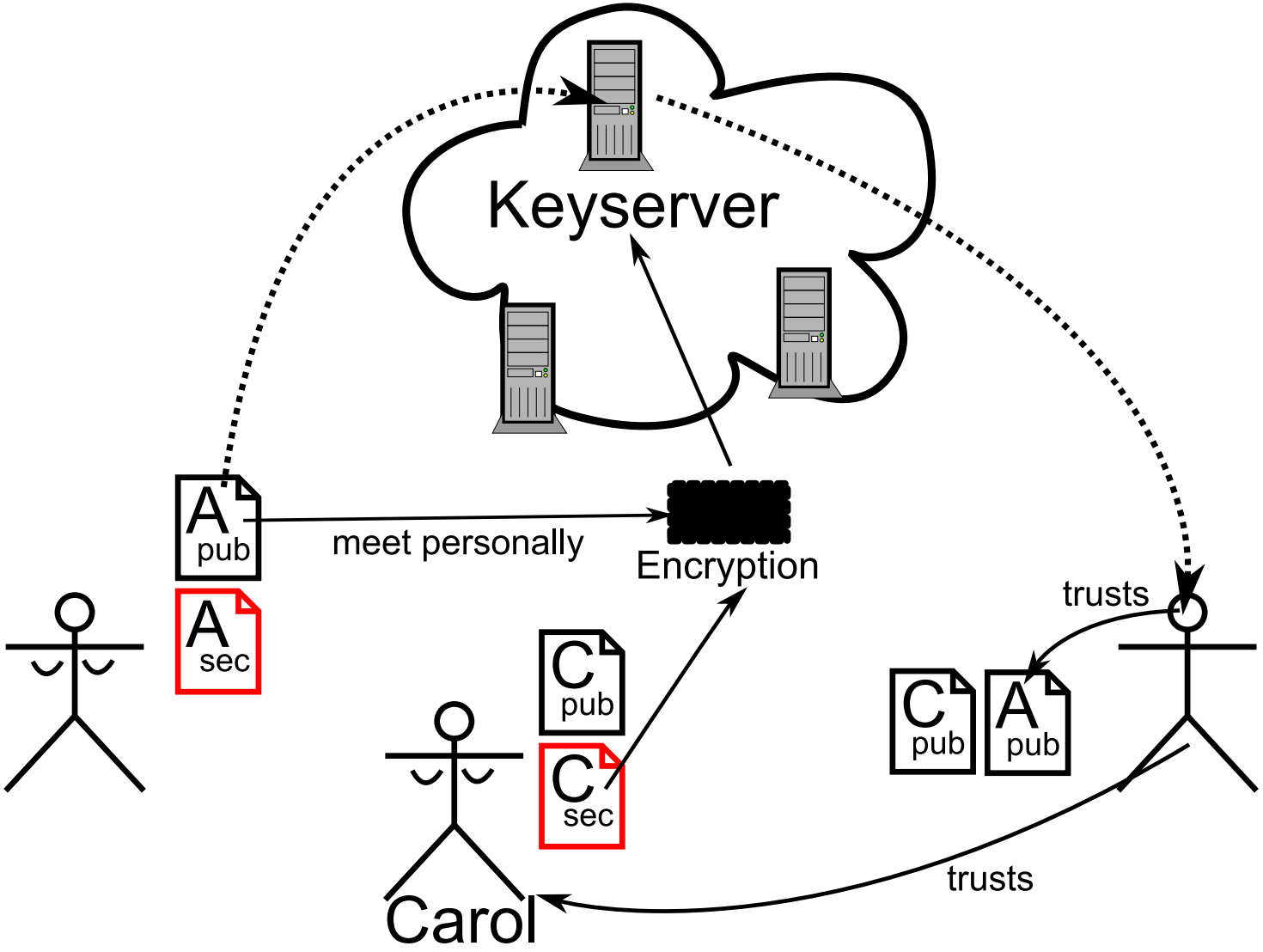
Key Signing



Key Signing


Keyserver
A
pub
A
sec
meet personally
Encryption
C
pub
C
sec
Carol
C
pub
A
pub
trusts

Key Signing


Keyserver
A
pub
A
sec
meet personally
Encryption
trusts
C
pub
C
sec
C
pub
A
pub
Carol
trusts

The GNU Privacy Guard

- 1991: "Pretty Good Privacy" by Phil Zimmermann
- 1994: Zimmermann founds PGP Inc.
- 1996: RFC1991, "PGP Message Exchange Formats"
- 1997: Network Associates Inc. bought PGP Inc.
- 1998: RFC2440, "OpenPGP Message Format"
- 1999: September 7th, GnuPG 1.0.0

The GNU Privacy Guard

- It's available for almost all operating systems; download from http://www.gnupg.org
- It works well from the command line!
- If you like something to click on: GPA, Seahorse, . . .
- Integration to many MUAs is available: mutt, Thunderbird + enigmail, . . .
- Documentation: (Fischer v. Mollard et al., 1999) (short); (Ashley, 1999) (long)

The GNU Privacy Guard

Demo!

GnuPG Smart Cards

- Key generation, encryption, decryption and signing on card (RSA, 1 kBit);
  keys never leave the card
- Stores three keys: generating signatures, encrypting data, authentication
- Stores various user specific and application specific data
- PINs may have up to 254 characters

GnuPG Smart Cards

- Documentation on how to use the cards with GnuPG is available at (Ehlers et al., 2005); card specification: (Pietig, 2004)
- GnuPG Smart Cards can be ordered from (Kernel Concepts, 2006).

Demo!

GnuPG Smart Cards

- Documentation on how to use the cards with GnuPG is available at (Ehlers et al., 2005); card specification: (Pietig, 2004)
- GnuPG Smart Cards can be ordered from (Kernel Concepts, 2006).

Demo!

Well, is it secure?

- Yes! Iff …
  - Encrypt as much as you can – this makes things pretty difficult for attackers since they don't know which mails are worth the effort.
  - Minimise the amount of not-encrypted copies of your data.

Well, is it secure?

- Yes! Iff …
  - Encrypt as much as you can – this makes things pretty difficult for attackers since they don’t know which mails are worth the effort.
  - Minimise the amount of not-encrypted copies of your data.

Well, is it secure? (cont'd)

- Yes! Iff . . .
  - Keep in mind that everything depends on the secrecy of your private key!
  - Use decent key sizes. 1 kBit isn't secure anymore.
  - Use proper pass phrases.
  - Store your keys on trustworthy systems only.
  - Do never use swodniW. It has no `mlock(2)`.

Well, is it secure? (cont'd)

- Yes! Iff . . .
  - Don't expect your data to be secure for more than 5 or 10 years.

Thank you!

Slides:

http://zeus.fh-brandenburg.de/~muehlber/ylug/crypto+gpg/crypto+gpg.pdf

References

Ashley, J. M.: 1999, *The GNU Privacy Handbook*, http://www.gnupg.org/gph/en/manual.html

Ehlers, R., Ehlers, T., Koch, W., and Kirschner, M.: 2005, *How to use the Fellowship Smartcard – The GnuPG Smartcard HOWTO*, http://www.gnupg.org/(en)/howtos/card-howto/en/smartcard-howto.html

Fischer v. Mollard, M., de Winter, B., Baart, A., and Cicek, B.: 1999, *Gnu Privacy Guard (GnuPG) Mini Howto*, http://webber.dewinter.com/gnupg_howto/english/GPGMiniHowto.html

Kernel Concepts: 2006, http://www.kernelconcepts.de/products/security-en.shtml

NASA: 2002, *A satellite composite image of Europe*, http://visibleearth.nasa.gov/view_rec.php?vev1id=11656

Pietig, A.: 2004, *Functional Specification of the OpenPGP application on ISO Smart Card Operating Systems*, http://www.g10code.de/docs/openpgp-card-1.1.pdf