Aalto University
School of Electrical
Engineering

Basic Principles in Networking

Digital signatures and End Point Authentication

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0

Aalto University
School of Electrical
Engineering

Video: INTERVIEW – Elliptic curve cryptography (10 min)

How did NSA read our emails?

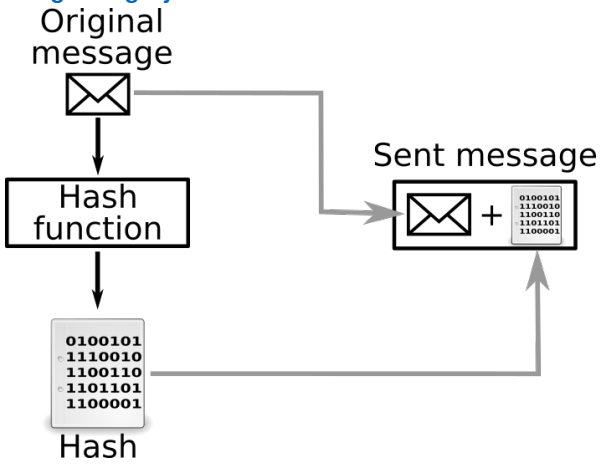
Aalto University
School of Electrical
Engineering

Part I (15 min)

Digital Signatures

Message Authentication codes

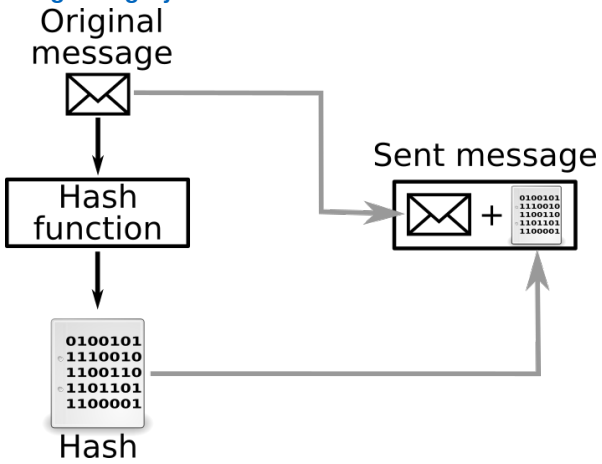
Use of hash functions to establish message integrity



Message Authentication codes

Use of hash functions to establish message integrity

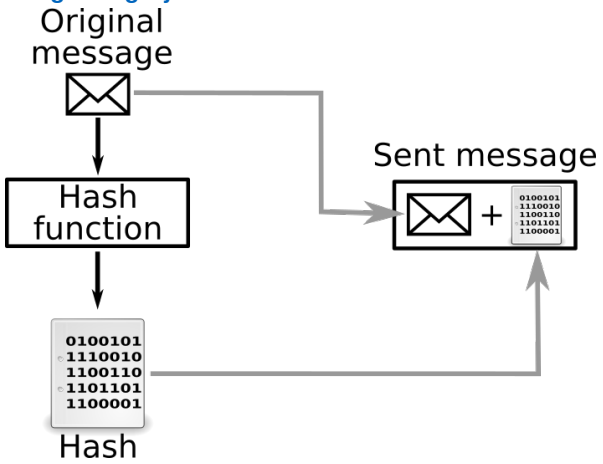
1. Create message m and calculate $H(m)$ (e.g. using SHA-2)



Message Authentication codes

Use of hash functions to establish message integrity

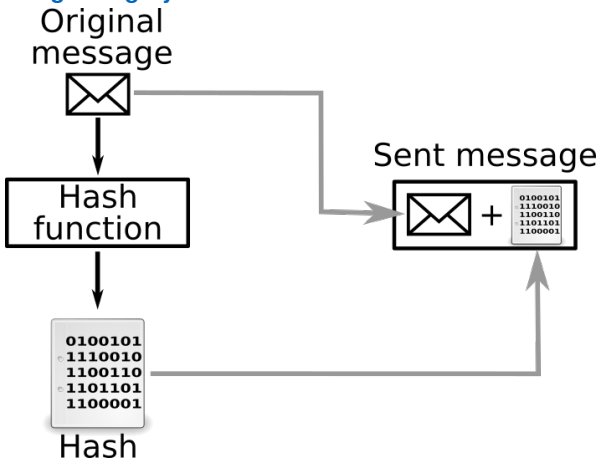
2. Create message m and calculate $H(m)$ (e.g. using SHA-2)
3. Append $H(m)$ to the message m and send $(m, H(m))$



Message Authentication codes

Use of hash functions to establish message integrity

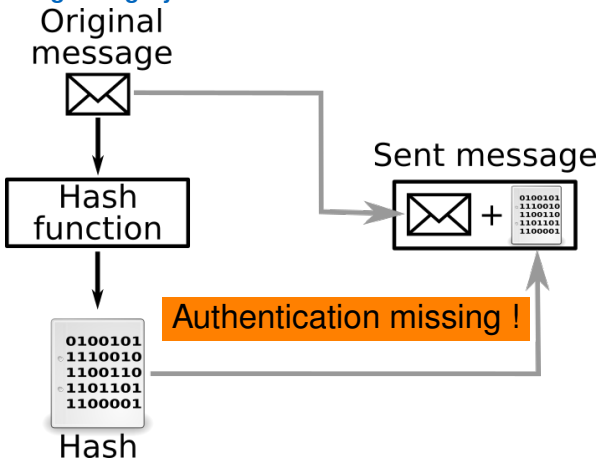
2. Create message m and calculate $H(m)$ (e.g. using SHA-2)
4. Append $H(m)$ to the message m and send $(m, H(m))$
5. Receiver of (m, h) calculates $H(m)$. Verify: $H(m) = h$



Message Authentication codes

Use of hash functions to establish message integrity

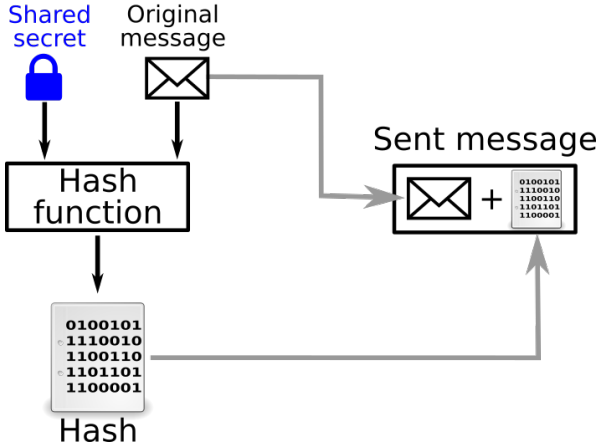
2. Create message m and calculate $H(m)$ (e.g. using SHA-2)
4. Append $H(m)$ to the message m and send $(m, H(m))$
5. Receiver of (m, h) calculates $H(m)$. Verify: $H(m) = h$



Message Authentication codes

Use of hash functions to establish message integrity

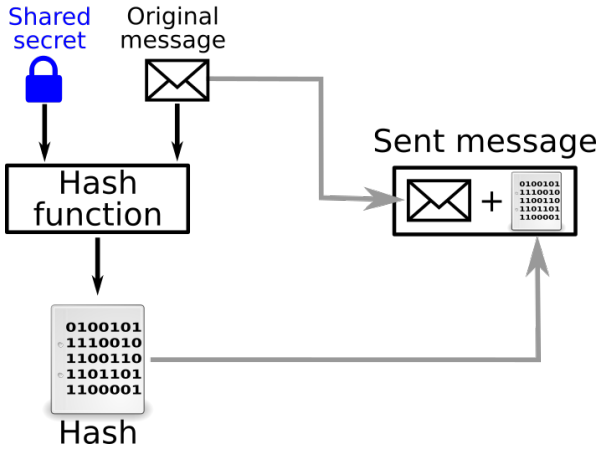
1. Create message m, concatenate $m + s$ and compute $H(m + s)$



Message Authentication codes

Use of hash functions to establish message integrity

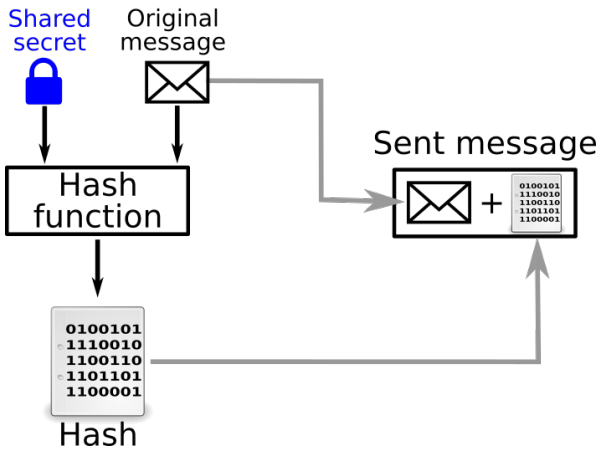
2. Create message m, concatenate $m + s$ and compute $H(m + s)$
3. Append $H(m + s)$ to m and send $(m, H(m + s))$



Message Authentication codes

Use of hash functions to establish message integrity

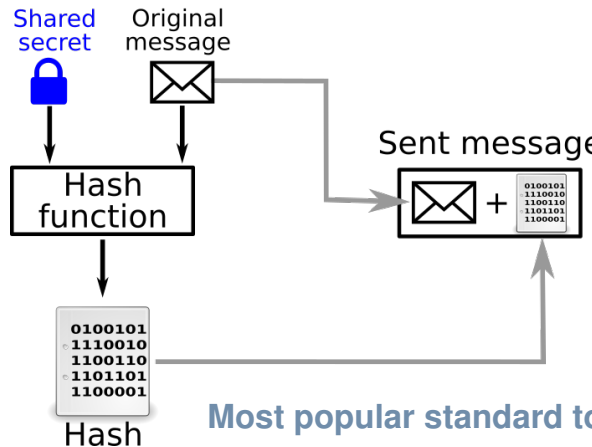
2. Create message m, concatenate $m + s$ and compute $H(m + s)$
4. Append $H(m + s)$ to m and send $(m, H(m + s))$
5. Receiver of (m, h) calculates $H(m + s)$. Verify: $H(m + s) = h$



Message Authentication codes

Use of hash functions to establish message integrity

2. Create message m, concatenate $m + s$ and compute $H(m + s)$
4. Append $H(m + s)$ to m and send $(m, H(m + s))$
5. Receiver of (m, h) calculates $H(m + s)$. Verify: $H(m + s) = h$



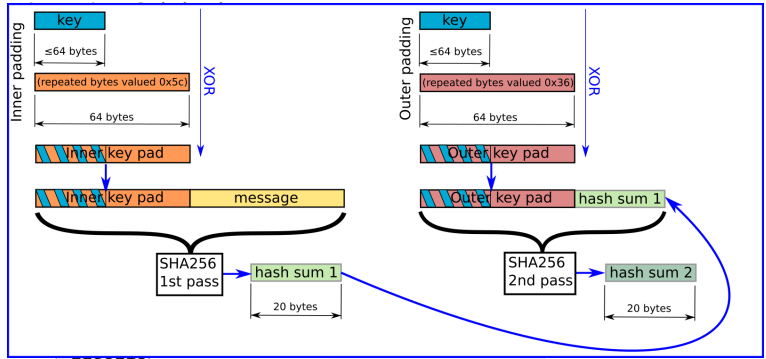
Most popular standard today: HMAC

Can be used with e.g. SHA-2/3

Message Authentication codes

Use of hash functions to establish message integrity

2. Create message m, concatenate $m + s$ and compute $H(m + s)$
4. Append $H(m + s)$ to m and send $(m, H(m + s))$
5. Receiver of (m, h) calculates $H(m + s)$. Verify: $H(m + s) = h$



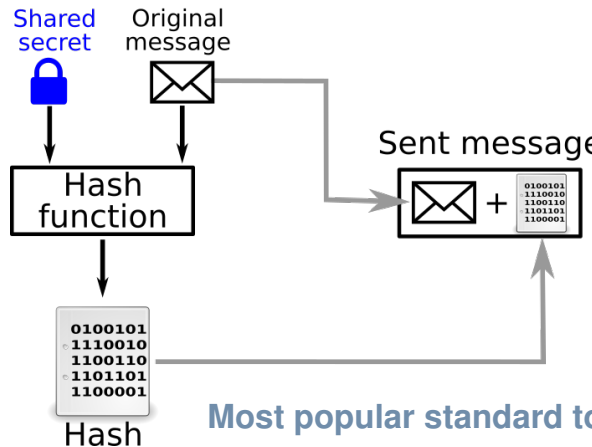
Most popular standard today: HMAC

Can be used with e.g. SHA-2/3

Message Authentication codes

Use of hash functions to establish message integrity

2. Create message m, concatenate $m + s$ and compute $H(m + s)$
4. Append $H(m + s)$ to m and send $(m, H(m + s))$
5. Receiver of (m, h) calculates $H(m + s)$. Verify: $H(m + s) = h$

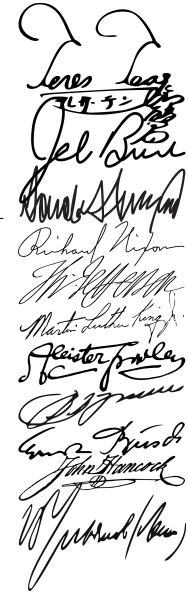


Most popular standard today: HMAC

Can be used with e.g. SHA-2/3

Digital signatures

A digital signature is a cryptographic technique to prove the identity of the owner/creator of a document or to signify one's agreement with a document's content



Digital signatures

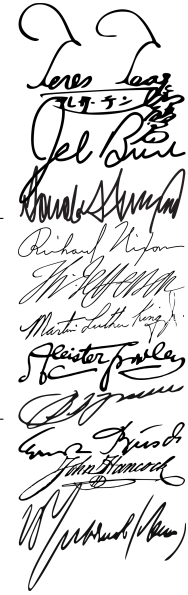
A digital signature is a cryptographic technique to prove the identity of the owner/creator of a document or to signify one's agreement with a document's content

---

Requirements for a digital signature

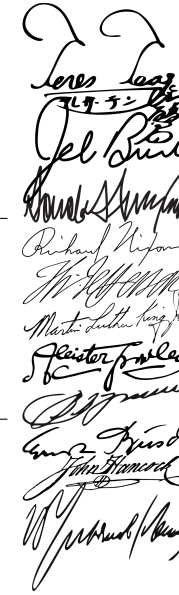
The signature must be unique to an entity in the network, verifyable and non-forgable

---



Digital signatures

A digital signature is a cryptographic technique to prove the identity of the owner/creator of a document or to signify one's agreement with a document's content



Requirements for a digital signature

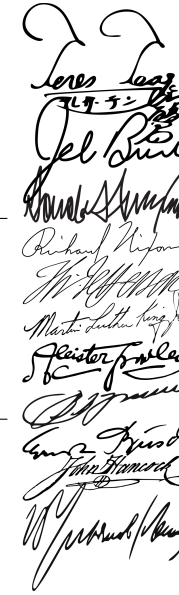
The signature must be unique to an entity in the network, verifyable and non-forgable

---

Can we use the message authentication code for the signature?

Digital signatures

A digital signature is a cryptographic technique to prove the identity of the owner/creator of a document or to signify one's agreement with a document's content



Requirements for a digital signature

The signature must be unique to an entity in the network, verifyable and non-forgable

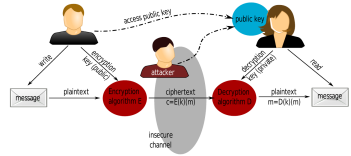
---

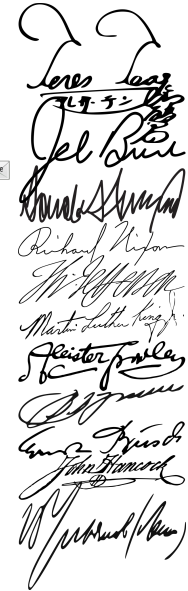
Can we use the message authentication code for the signature?

No: To verify the signature, the receiver needs a copy → not unique

Digital signatures

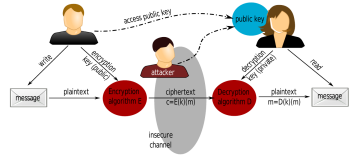
Asymmetric encryption for Digital Signatures

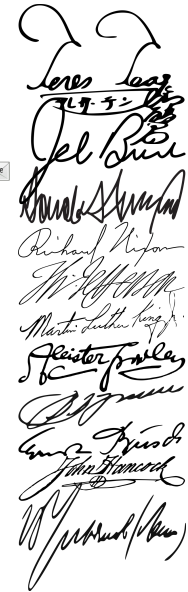




Digital signatures

Asymmetric encryption for Digital Signatures

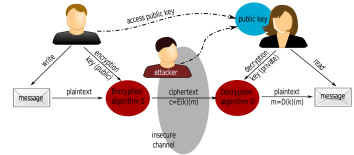




Signature is created by encrypting the message m with the private key: $K_B^-(m)$

Digital signatures

Asymmetric encryption for Digital Signatures

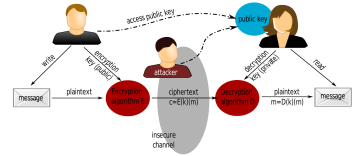


Signature is created by encrypting the message m with the private key: $K_B^-(m)$

Private key K_B^- unique to sender and can be verified by anyone with the public key: $K_B^+(K_B^-(m)) = m$

Digital signatures

Asymmetric encryption for Digital Signatures



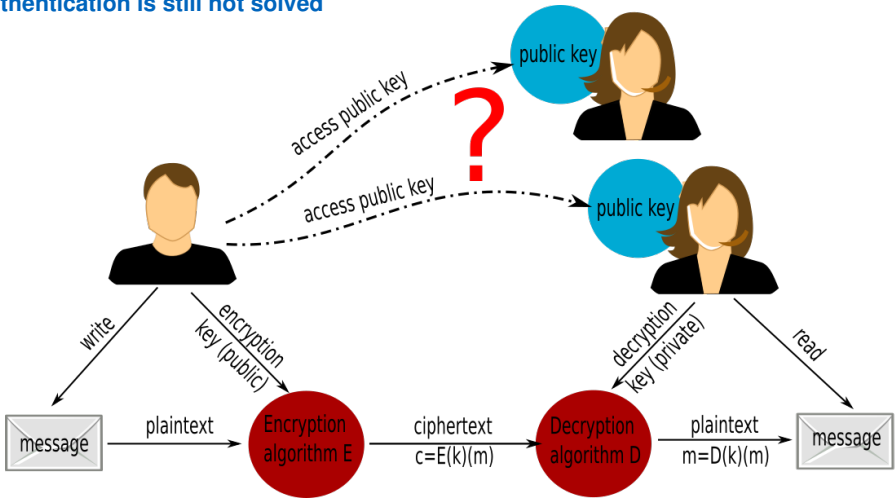
Signature is created by encrypting the message m with the private key: $K_B^-(m)$

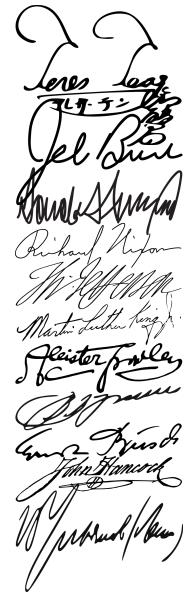
Private key K_B^- unique to sender and can be verified by anyone with the public key: $K_B^+(K_B^-(m)) = m$

Non-forgable since it is *not computationally feasible* to find m' with $K_B^+(K_B^-(m)) = m'$

Digital signatures

Authentication is still not solved





Aalto University
School of Electrical
Engineering

Part II (10 min)

End-point authentication

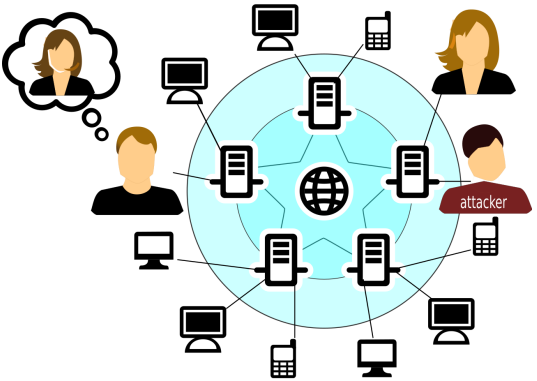
End-point authentication

Why is authentication difficult in networks?

End-point authentication

Why is authentication difficult in networks?

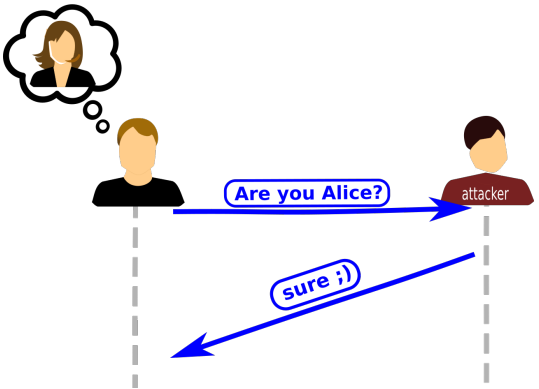
⇒ Unlike face-to-face communication, other party is 'invisible'



End-point authentication

Why is authentication difficult in networks?

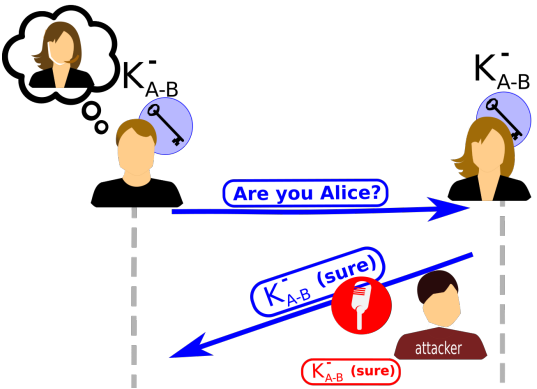
⇒ Unlike face-to-face communication, other party is 'invisible'



End-point authentication

Why is authentication difficult in networks?

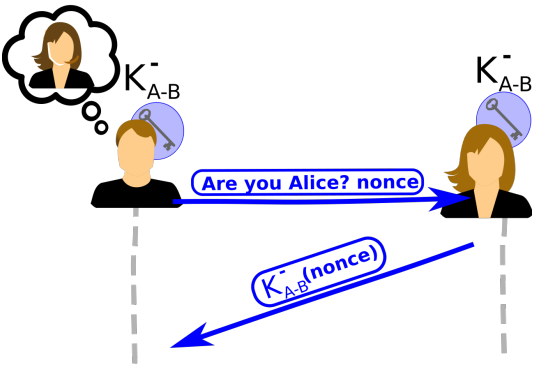
- ⇒ Unlike face-to-face communication, other party is 'invisible'
- ⇒ Replay attacks



End-point authentication

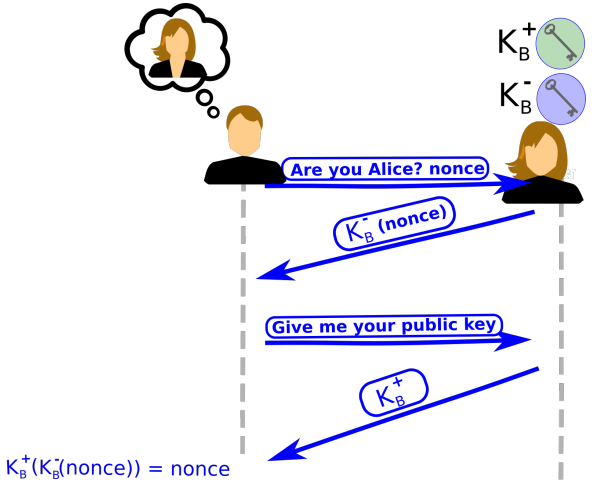
Why is authentication difficult in networks?

- ⇒ Unlike face-to-face communication, other party is 'invisible'
- ⇒ Replay attacks



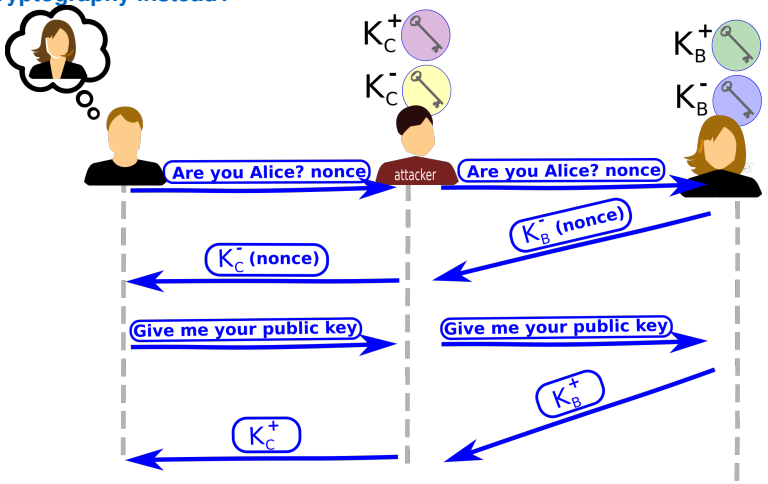
End-point authentication

Use asymmetric cryptography instead?



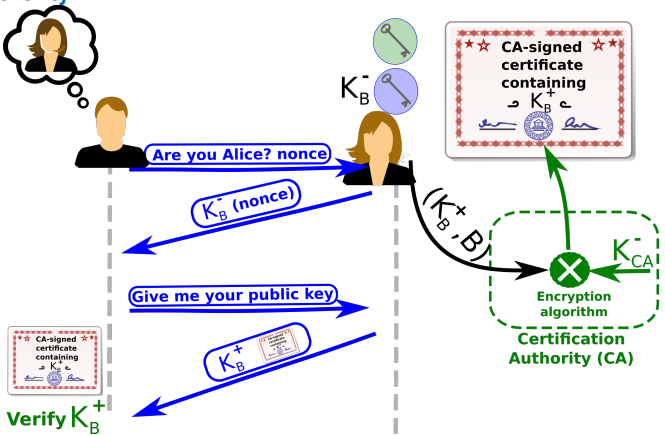
End-point authentication

Use asymmetric cryptography instead?



End-point authentication

Solution: Certified Authority



$\Rightarrow$ CA issued certificate contains K_B^+, B; digitally signed by K_{CA}^-

Aalto University
School of Electrical
Engineering

Video: RSA 2016 – cryptographers panel (10 min)

Impact of the NSA-incident

Questions?

Stephan Sigg
stephan.sigg@aalto.fi

Esa Vikberg
esa.vikberg@aalto.fi

Leo Lazar
leo.lazar@aalto.fi

Literature

- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (7th edition), Pearson, 2016.
- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (6th edition), Addison-Wesley, 2012.