Computer Networks

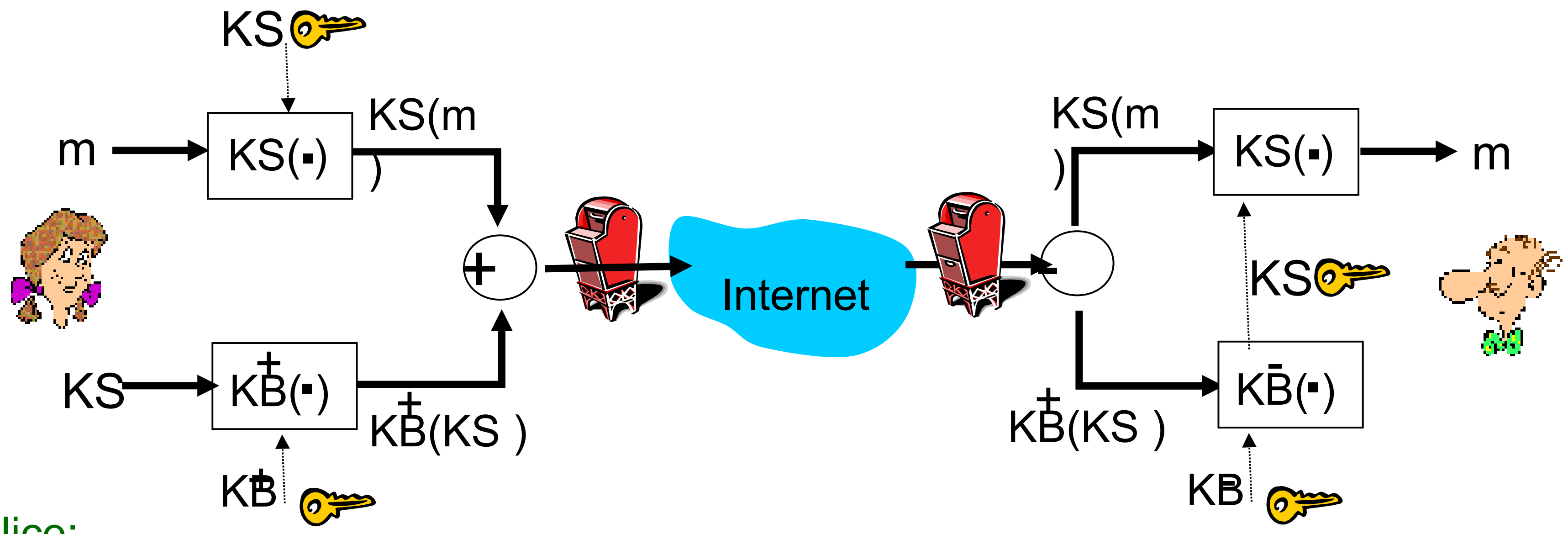
Exercise 12

Announcements

- Final exam: Thursday 06.02.2014
    - 10:00 -12:00 : MN06
- Language: English + German, answers possible in both languages

- No additional resources (calculator etc.) allowed. Just bring pens ;).

Secure E-Mail



Alice:

- generates random *symmetric* private key, KS.
- encrypts message with KS (for efficiency)
- also encrypts KS with Bob's public key.
- sends both KS(m) and KB(KS) to Bob.

Bob: uses his private key to decrypt and recover KS

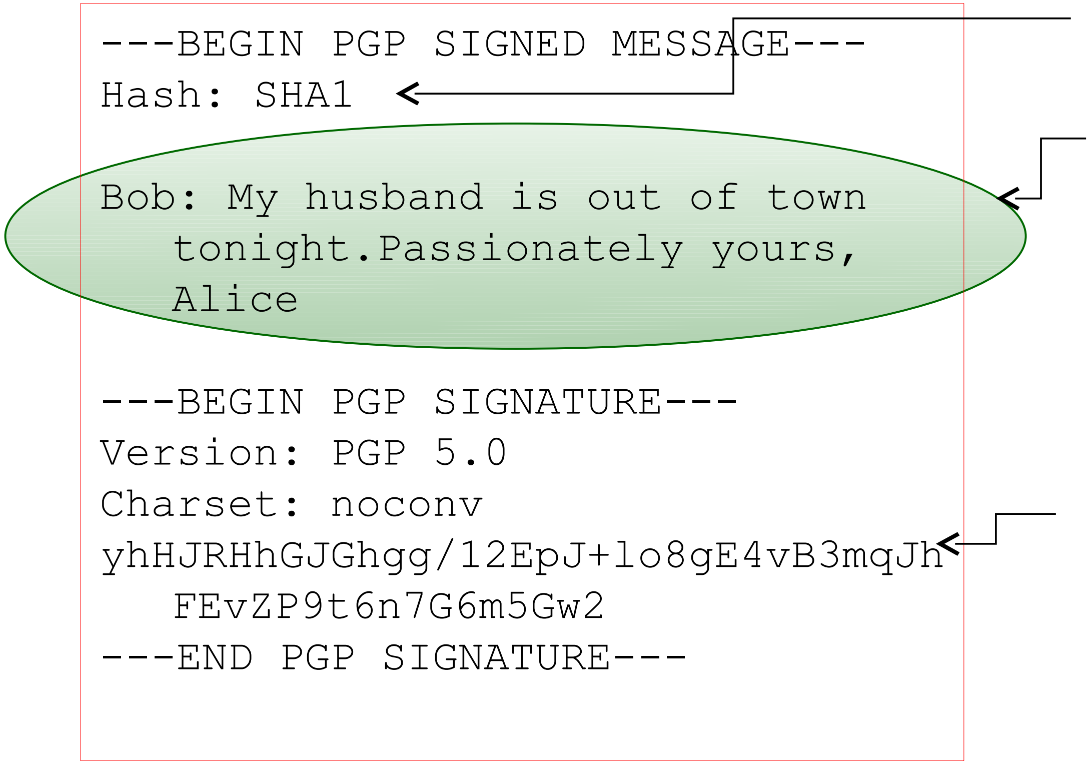
- uses KS to decrypt KS(m) to recover m

Why symmetric keys?

- Why is a symmetric key used in most protocols to encrypt a data payload (the message etc.), even if a public/private key infrastructure exists?

- Public/Private keying more costly
- Minimal use of public/private key minimizes the key exposure
  - Symmetric key can be generated each time on the fly and is therefore always fresh
  - Public/Private key is always the same. Encrypting large amounts of data could compromise the key... (although no efficient algorithm is known yet)

PGP E-Mail signature



```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob: My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJh
   FEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Used crypto hash

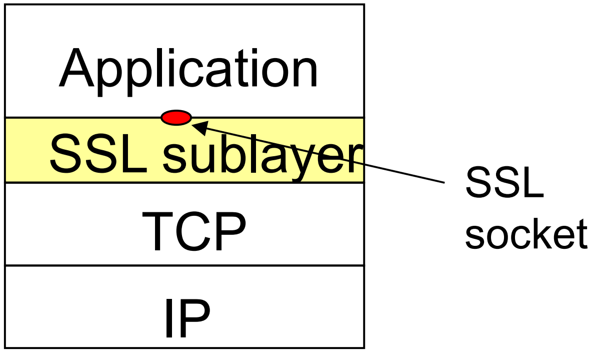
Message m that is hashed with SHA1

Real signature: This is the hash of the message (H(m)) encrypted with Alice’s private key.

Verification: Bob decrypts the PGP signature and obtains H(m). Additionally he computes H(m) for the message himself and computes it with the H(m) Alice computed.

SSL

- What are the three main phases of SSL?
  - 1. Handshake (TCP connection, authentication + master secret generation)
  - 2. Key derivation
  - 3. Data transfer
- On what layer does SSL reside and why is that advantageous?
  - provides transport layer security to any TCP-based application using SSL services.



TCP enhanced with SSL

IPsec

- Please sketch one typical scenario, where IPsec is used today.
    - VPN gateway at company or university. E.g. 134.76.22.1 is the VPN Gateway for the GWDG
    - Note: IPSec works on IP layer (SSL: above TCP)
- What are the two main protocols used in IPsec and what is their primary difference with respect to security properties?
    - Authentication Header (AH): Ensures authentication and data integrity. No encryption!
    - Encapsulated Security Payload (ESP): Ensures authentication, data integrity and encryption.

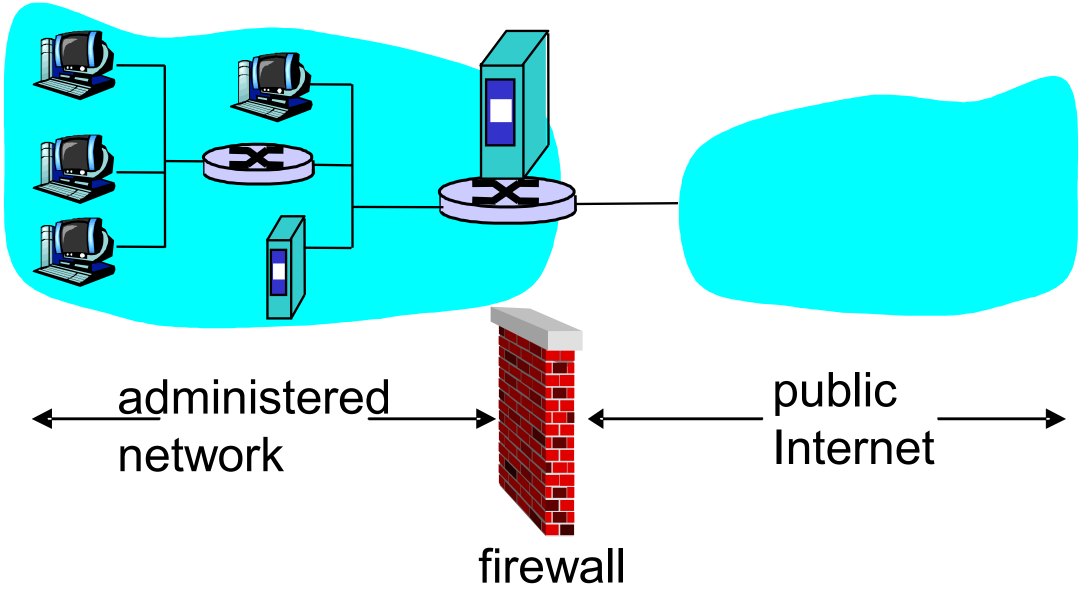
802.11i

- Should ensure better protection than WEP
  - WPA is a subset of 802.11i

- Who is handling the authentication information in an 802.11i scenario?
  - Using TLS-EAP (Extensible Authentication Protocol over Transport Layer Security) to contact an AAA (Authentication, Authorization, Accounting) Server

Firewalls

- What is the purpose of a firewall and what are filter rules?
  - Isolation of own network from internet!



Filter rules

- The firewall can be configured to only let certain packets pass. An administrator might be interested in setting up rules like:
    - No telnet connections to hosts behind the FW
    - Prevent outside machines to connect to inside machines, but still inside machines can connect to outsiders
    - Prevent web radios
    - Many more…

Thank you

Any questions?