# MTAT.07.017
# Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

# Topics for This Week

Public Key Cryptography

Java Cryptography Architecture:

- `java.security.KeyPair`
- `java.security.KeyPairGenerator`
- `java.security.Signature`

# Symmetric Cryptography

```
encrypt(msg, K) = ciphertext
decrypt(ciphertext, K) = msg
```

Key size: 80..128 bits

Simple and fast

# Symmetric Cryptography

Message authorship identification

- Not possible: each key exists in at least 2 copies

Key management hell

- How many keys needed?
- How to transport keys?

# Public Key Cryptography

Key pair instead of a single key: **K+** ≠ **K-**

```
encrypt(msg, K+) = ciphertext
decrypt(ciphertext, K-) = msg
```

Key size: 1024..4096 bits

Tricky and slow

# Public Key Cryptography

Key management issues: solved (mostly)

- **2N** keys needed for N parties
- Public keys can be sent via insecure* channels

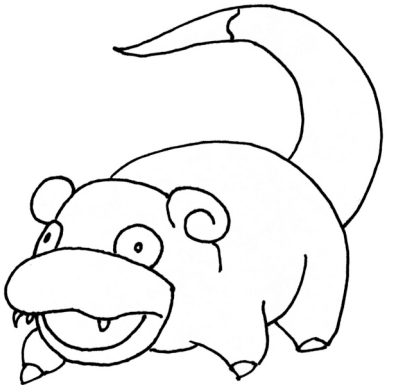
  * We should still be able guarantee sender authenticity
- Private keys are not sent anywhere

Both sender and recipient can be identified

# Public Key Cryptography

Encrypting with public key algorithms is slow

Very slow



Usage:

- Digital signatures
- Key exchange in hybrid cryptosystems

# Digital Signatures

Private key **K-** to sign a message (encrypt)

Public key **K+** to verify signature (decrypt)

Only digest is signed – not the entire message

```
sign(hash(msg), K-) = signature
verify(signature, K+, hash(msg))
```

# Digital Signatures

Sender authentication & non-repudiation

Data integrity

DSA (Digital Signature Algorithm)

http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

RSA (Rivest/Shamir/Adleman) algorithm

http://en.wikipedia.org/wiki/Rsa

# Hybrid Cryptosystems

Public key algorithms to exchange symmetric keys

Symmetric algorithms to encrypt and decrypt data

PGP and GPG

- http://en.wikipedia.org/wiki/Pretty_Good_Privacy
- http://en.wikipedia.org/wiki/GNU_Privacy_Guard

TLS (Transport Layer Security) Handshake

- http://en.wikipedia.org/wiki/Transport_Layer_Security

# Questions?

```
import tasks3;
```

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab03

# Questions?

# Good Luck!

Tasks, exercises, additional info:

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab03

**Deadline: 2011-03-11 08:00 EET**

Contact: Juri Hudolejev <juri@ut.ee>

Next lab session:

Friday 2011-03-11 **08:30** EET @ Liivi 2 - 205