PV018 – IT Security Seminar

Advanced Topics in IT Security

Vašek Matyáš

Email: matyas@fi.muni.cz

Office hours: Mon & Wed 12:00-13:00 (B415)

Marking Your Performance

- 40% - written exam (closed book).
- 30% - term project :
  - Topic of your choice, approved by the lecturer!
  - Worth about 30 hours of work.
  - Final report (5-7 pages) submitted by May 25th.
- 30% - assignments (3-4) through the term:
  - Deadline in 10-14 days.
  - Distributed and collected electronically.

The Final Mark

A for 90% or higher, then
B for 80% or higher, then
C for 70% or higher, then
D for 60% or higher, then
E for 50% or higher, then
F(ail) for less than 50%.

Colloquy or credit – at least 50% needed.

Marking & Language

- The course and assignments are given in English.
- Questions (course, assignment, etc.) should be in English.
- Assignments are to be handed in also in English!!!
- Final exam and the term project are accepted in both Czech and English.

Course topics I.

- Authentication
  - of users – tokens, biometrics…
  - of data – cryptographic means – digital signatures, MACs
- Applications of cryptographic mechanisms, especially of the public key techniques
- Block ciphers and modes of operation
  - AES, DES
- Key management and protocols
  - Public-key infrastructures

Course topics II.

- Internet security
- Biometrics – relations to cryptography.
- Role of standards and evaluation (criteria).
- Secure hardware.
- Risk assessment and evaluation
- *Up-to-date topics are also set during the term.*
  - *Open to suggestions!*

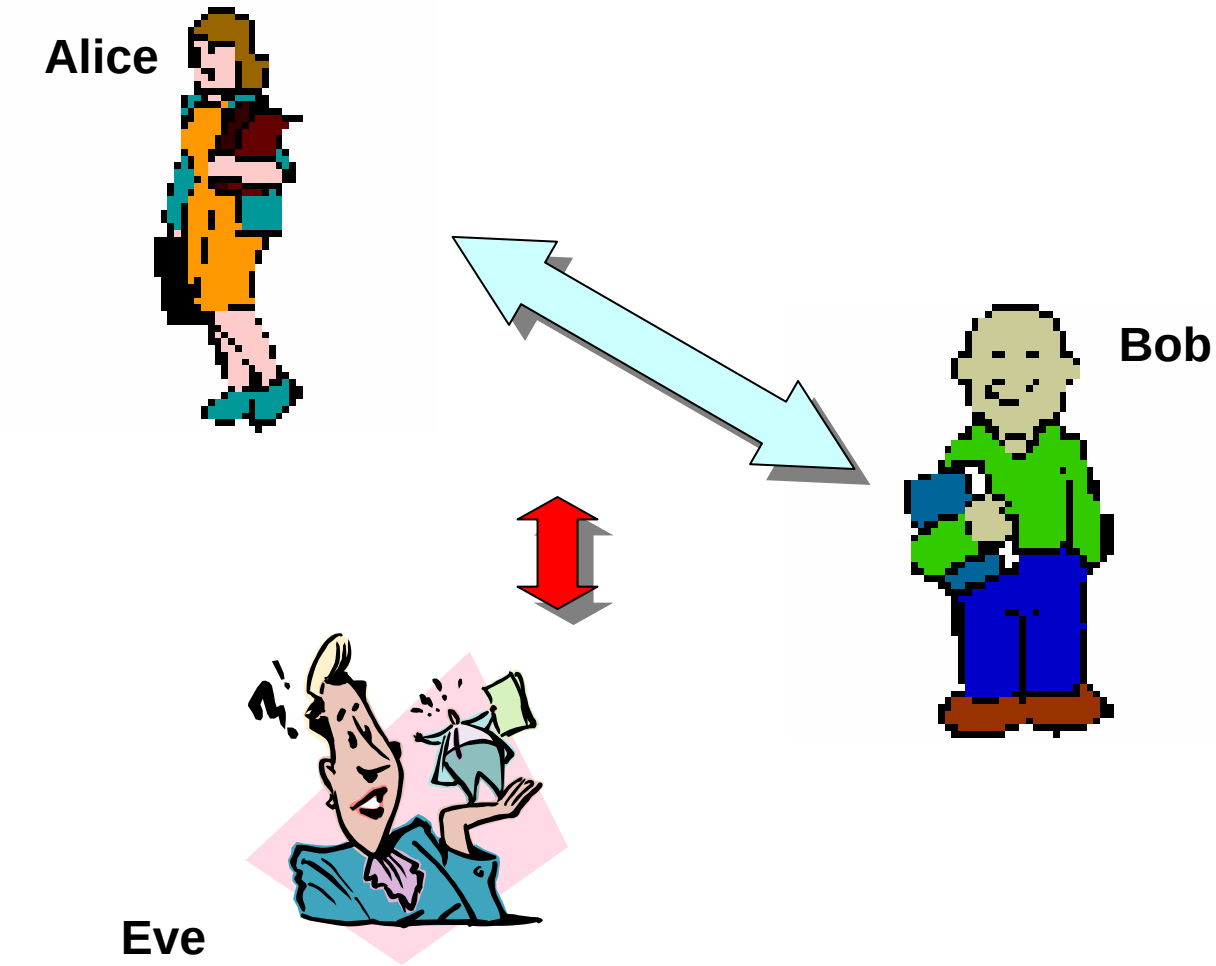
Typical Security Requirements I.

- **Authentication**: originator's identity assured.
- **Integrity**: information received as originated.
- **Confidentiality**: information available only to authorized parties.

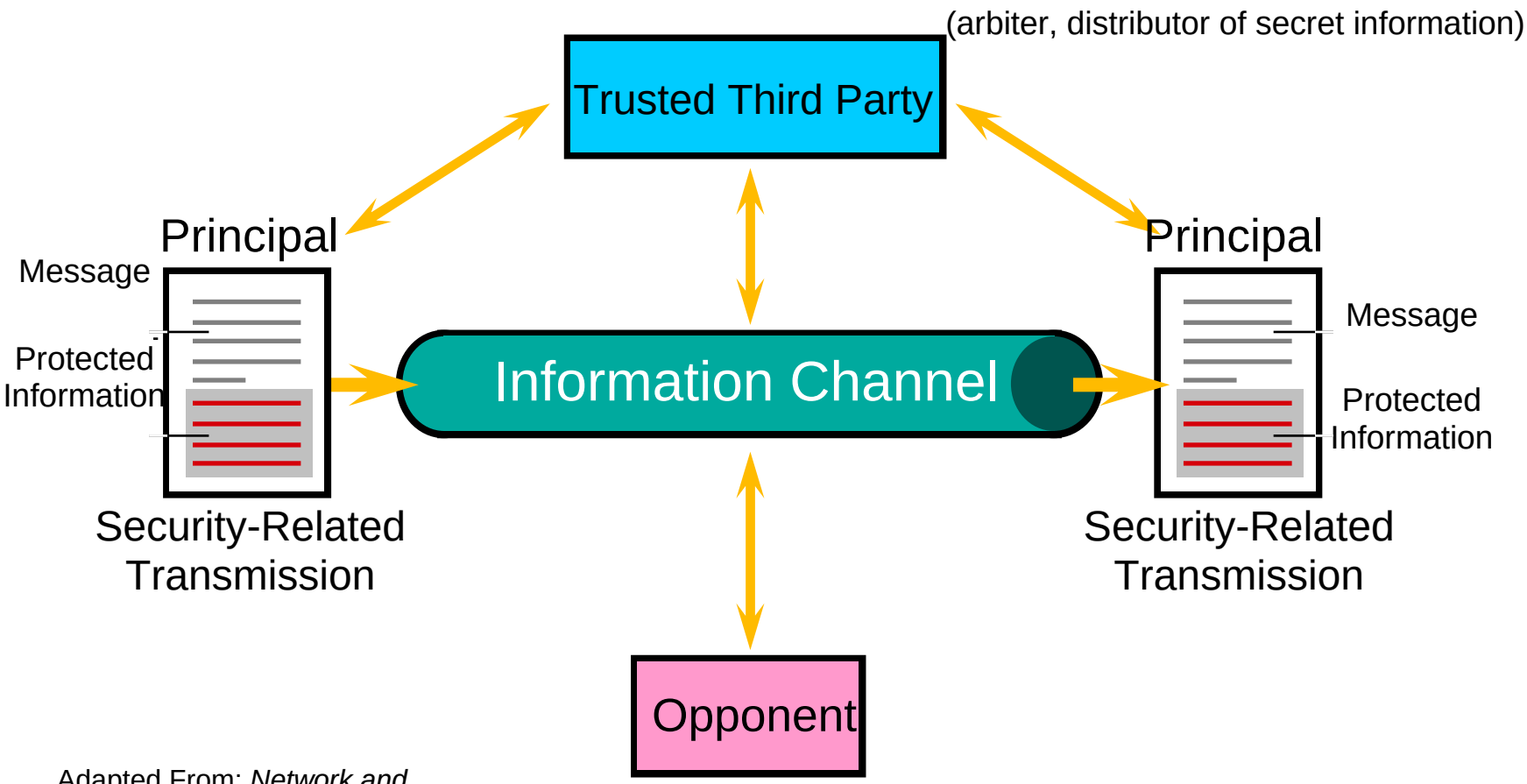
Typical Security Requirements II.

- **Availability**: data & resources available when needed.
- **Non-repudiation**: party cannot deny communication (origin, receipt, delivery, etc.).
- **Access Control**: resources controlled by authorized parties.
- …could list a few more…

Conventional Names for Players



Network Communications Security Model



Adapted From: *Network and Internetwork Security* (Stallings)

What are keys?

- Large bitstrings
  - random numbers
- Symmetric Cryptography
  - Same Key for Alice and Bob
- Asymmetric Cryptography
  - Private Key (Confidentiality)
  - Public Key (Integrity)

...000100101010
01010100010100
10010101001001
00010111110101
01110101011100
10101100101000
10101001010010
10101011111101
10100110010001
00111010101010
110...

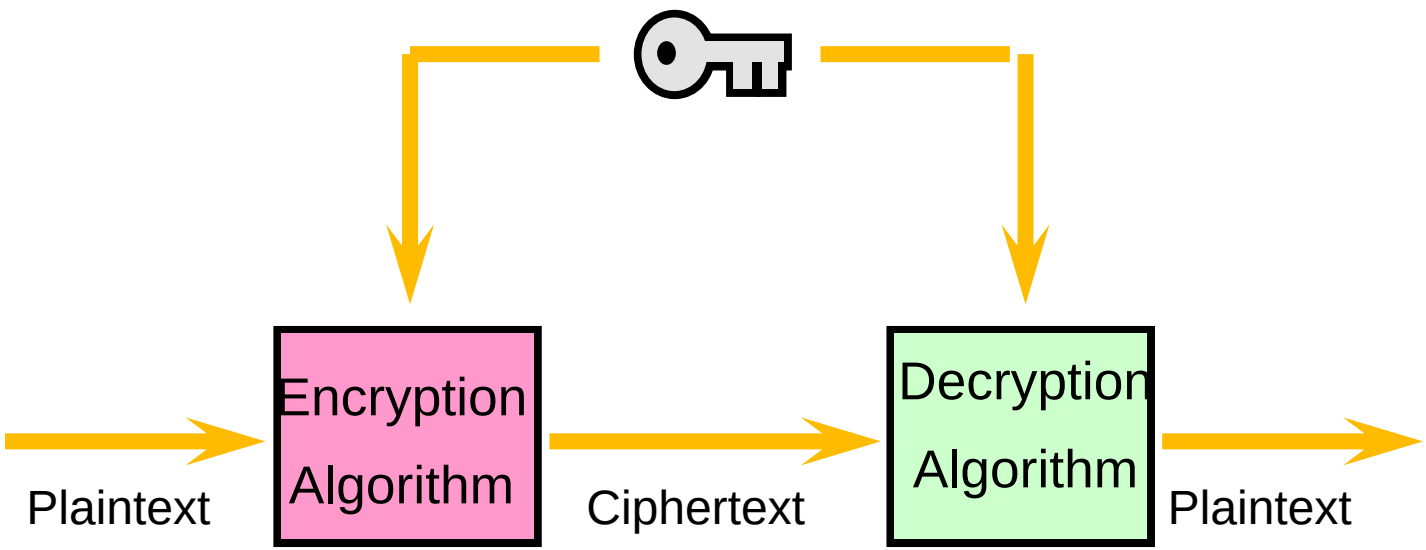
What is hashing?

- “Data Fingerprints”
  - short & unique image of data
- 01:A0:7D:2B:76:52:67:05
- EC:43:6F:B3:68:CE:20:E7

- Hashing functions
  - one-way, collision-free
  - SHA-2 series (256bit and more)
  - „retiring“ SHA-1 (160b),
  - „retired“ MD5 (128b)

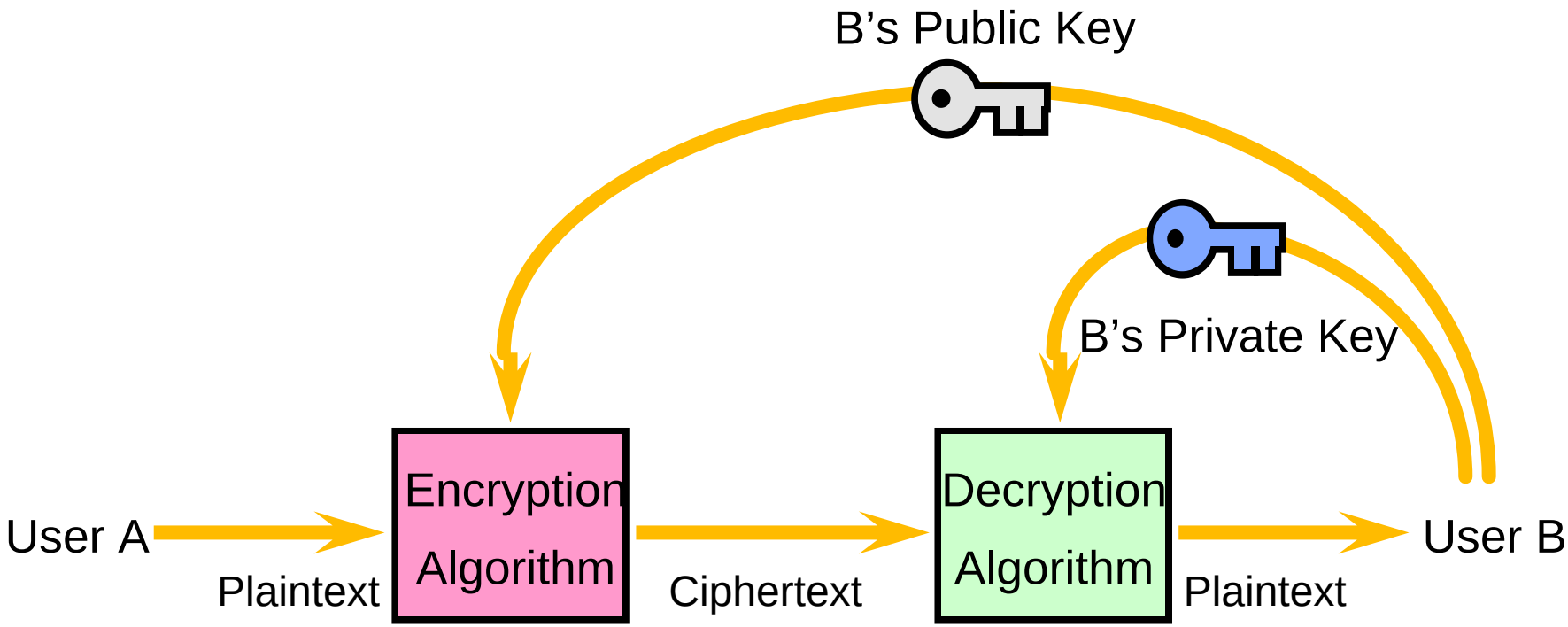
… It will be a blustery day for Scotland with gales and showery rain in the north-east. Elsewhere in Scotland the showers will be more scattered at first with a few sunny spells, but outbreaks of rain will spread from the south-west this afternoon. Northern Ireland, Wales and England will also have a showery day. The showers are likely to merge to give longer spells of rain at times, although in the south and west there is a better chance of some sunny intervals this.…

Simplified Model of Conventional Encryption



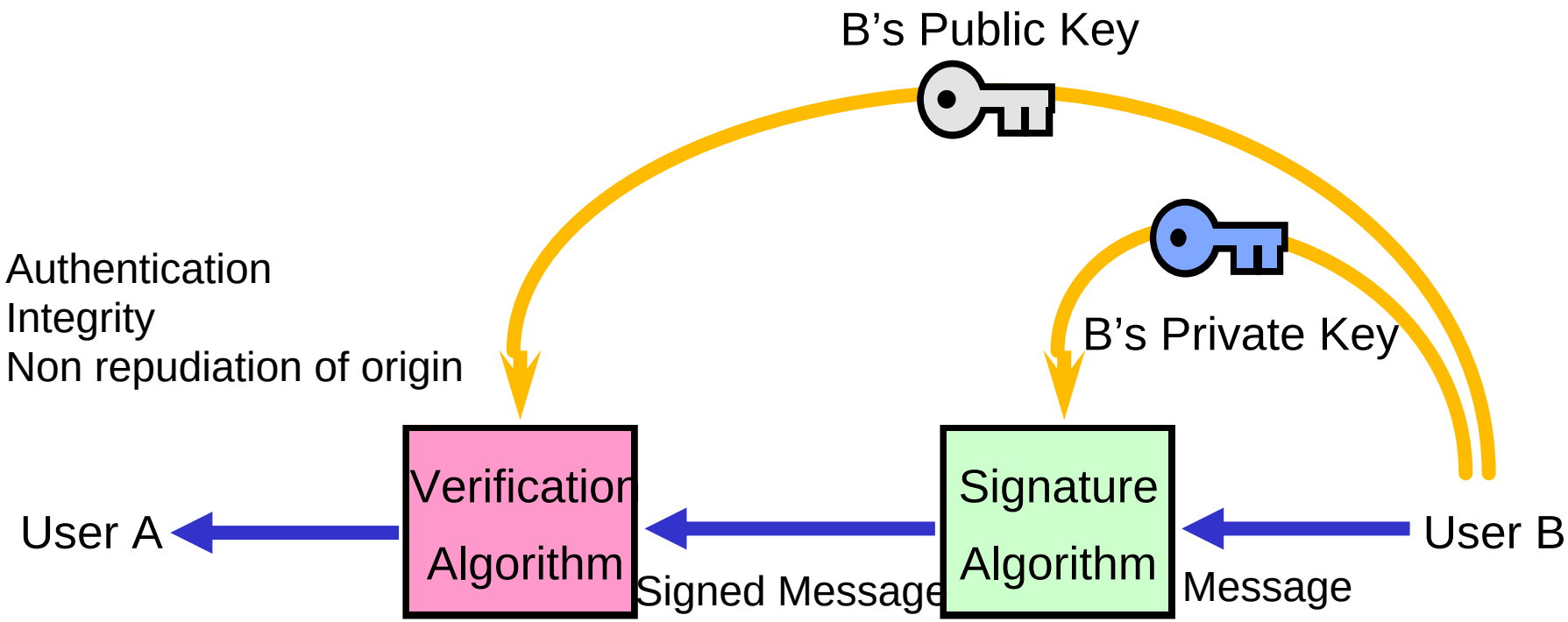
Adapted From: *Network and Internetwork Security* (Stallings)

Simplified Model of Public-Key Encryption



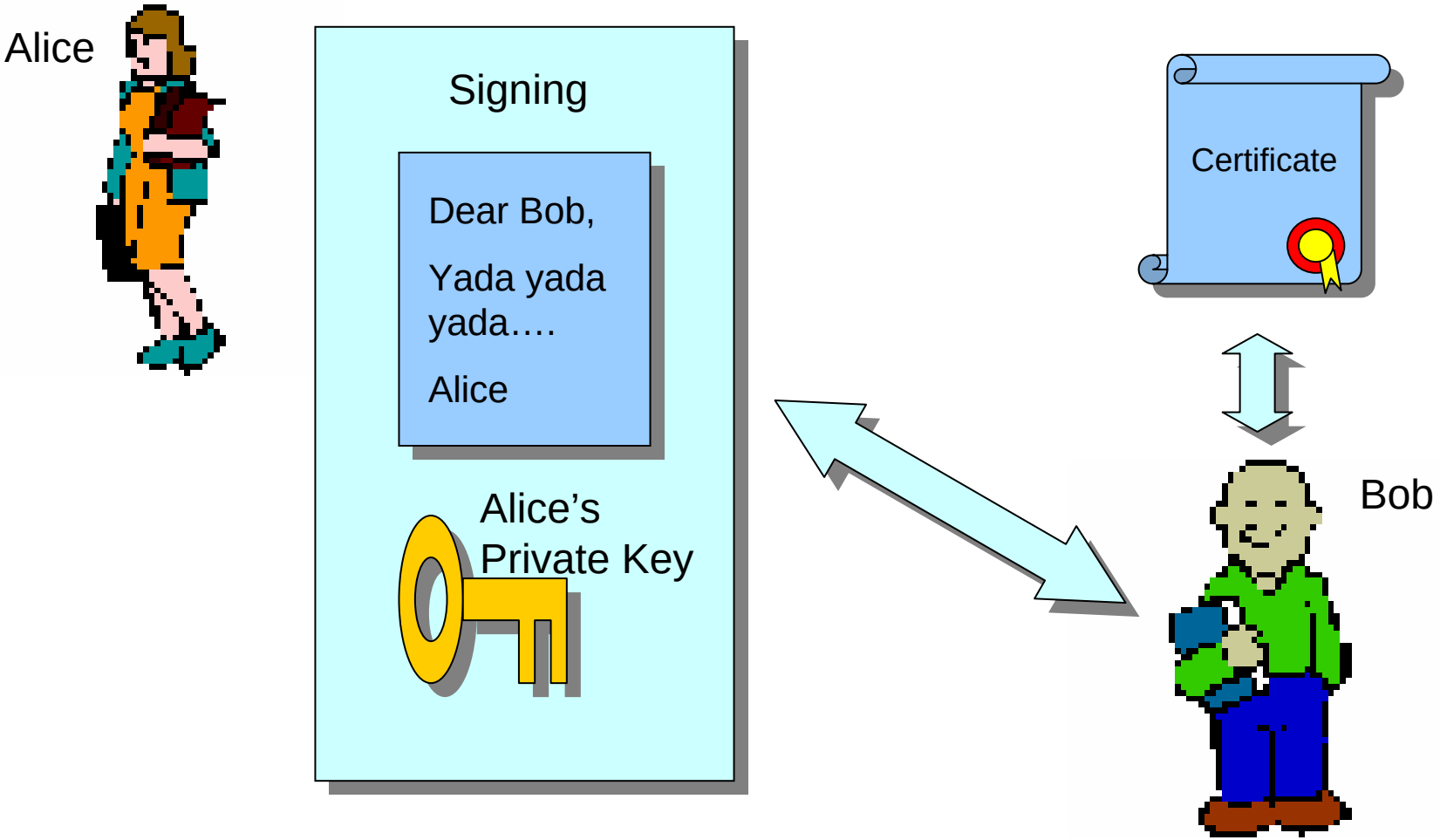
Adapted From: *Network and Internetwork Security* (Stallings)

Simplified Model of Public-Key Signatures



Adapted From: *Network and Internetwork Security* (Stallings)

What are Digital Signatures?



Generic security goals - Protection against…

- access to information by unauthorized parties
- modification of data by unauthorized parties
- unaccountable modification/deletion/creation… of data by unauthorized parties
- withholding data or resources from authorized parties
- false denial of a party's involvement in a given action
- …

Security is not just prevention

1. Prevention (protection)
2. Detection
3. Reaction

Information dominance

1. Aim: Reaching own information dominance: having the right information at the right place in the right time.

2. Aim (offensive): Limit the other party in reaching full information dominance.

One after another…

1. Risk analysis
2. Specification of security policy and security architecture
3. Design and implementation of security mechanisms
4. Support, maintenance, control, re-evaluation (back to 1…)

Security policy

- VERY IMPORTANT for improving the (IT) security in any company
- Company *business goals* → IT goals → IT security goals
- Helps with
  - Setting priorities (for IT, security departments)
    - Long-term goals vs. short-term goals
    - Improvement of services (vs.) company survival(!)
  - Getting management support and assuming direct responsibilities

Trusted (system, component…)

- Such one that behaves in a way we expect it to behave
- Can be trusted to only such a functionality that adheres to the relevant security policy
- Trust
  - Belief that (a system…) satisfies given (security) requirements and specifications
  - Chance that (a system…) can breach the (security) policy without leaving any trace of evidence ☺

Accident and attack

- Murphy's Law
  - bad things can happen by accident,
  - and we should expect that they will happen, preparing for a malfunction
- Satan's Law
  - very bad things can happen at someone's will
  - and we should do our best to consider all possible ways of pursuing that will, preparing for an attack
- B. Schneier – see Crypto-Gram (ref. later)

Threat exploits vulnerability…

- **Vulnerability –** A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy.
- **Threat –** Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, denial of service…

Risk helps us judge threat…

- **Risk –** The probability that a particular threat will exploit a particular vulnerability of the system.
- **Risk analysis –** The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Attack – the threat comes true…

- **Attack –** The act of trying to bypass security controls on a system. An attack may be active, e.g. resulting in the alteration of data; or passive, e.g. resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

Authenticate & Authorize

- **Authenticate –**
  1. To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
  2. To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.
- **Authorization –** The granting of access rights to a user, program, or process.

Incidents caused by

- Errors (not intended to happen): 50-70%
- Natural/utility influence: 10-15%
- Malicious software: 5-10%
- Intentional sabotage/attack/corruption by own/past employees/members: 10-20%
- External attackers: 1-5%

Impact of incidents is yet another issue!

Security policy and company culture

- The best security mechanisms are useless without effective support of all parties involved
- End-users must be trained and interested
- Management must be involved (or better lead!)
- Security is a process, not a product

Role of IT security manager

- Experience with IT security very important
- Art of persuasion critical!
- Experience: 60% management skills, 40% security expert skills
- Very demanding and challenging position
  - Criticized for incidents
  - Criticized for obstructions to “normal” processes
  - Can be appreciated for “nothing happening”? ☺

Crypto-Gram Newsletter

- Free monthly e-mail newsletter on general and computer security from Bruce Schneier (author of Secrets and Lies and Applied Cryptography, inventor of Blowfish and Twofish, CTO and founder of Counterpane Internet Security…).
- *http://www.schneier.com/crypto-gram.html*

The RISKS Forum

- The RISKS Forum is a moderated digest. Its USENET equivalent is *comp.risks*.

- *http://www.risks.org*

Recommended reading – week 1

- **Why Cryptosystems Fail, R. Anderson**
- 1993 paper with results of a survey of the failure modes of retail banking systems, with criticism of the threat model commonly used by cryptosystem designers: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures.

- *http://www.cl.cam.ac.uk/users/rja14/wcf.html*

Topics for term projects

- New trends in… firewalls, IDS, mobile security, viruses…
- Study of… a virus, a particular security solution/system, crypto algorithm…
- Security of … Java, HTTP authentication…

Deadline for proposal *and approval* – March 9!!!

Questions, comments, suggestions…???

Go ahead!

☺

Seeking researchers…

- Bc thesis
  - *Ovlivňování generátorů skutečně náhodných sekvencí v kryptografických čipových kartách*
- MSc thesis
  - *Generování pseudonáhodných sekvencí v kryptografii*
- Both can lead to scholarship award in 2-3 months