PA018 –
Advanced Topics in IT Security

Vašek Matyáš

Email: matyas@fi.muni.cz

Office hours: Mon 15:05-55 & Tue 9:05-55 (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 (excl. doc. editing).
  - Final report (9-10 pages) submitted by May 22nd.
- 30% - assignments (approx. 5) 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%.

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, as should be the project presentation!!!
- Final exam and the term project are accepted in both Czech and English.

Structure of the course

- First half-term of lectures and readings
  - Readings – seminal papers in the field
  - …and work on the term project!!!
  - Rather demanding work, compensating for the end of the term
- 3-4 guest lectures (fingerprints and liveness, HSMs, malware and firewalls / networks)
- May (after Easter)
  - **your** term project presentations
    - Part (5 of 30 points) of your mark
    - With feedback to reflect in the final report

Typical Security Requirements I.

- **Authentication**: originator’s identity assured.

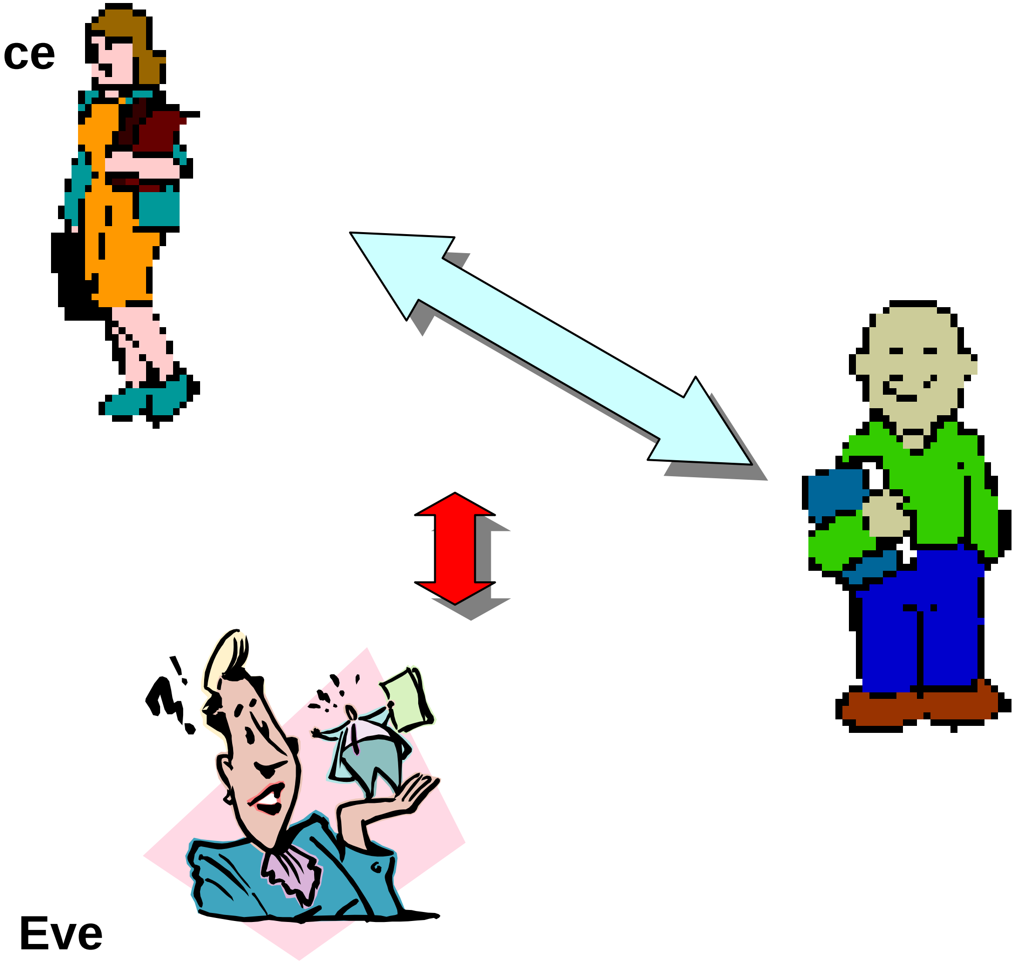
- **Integrity**: information received as originated.

- **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

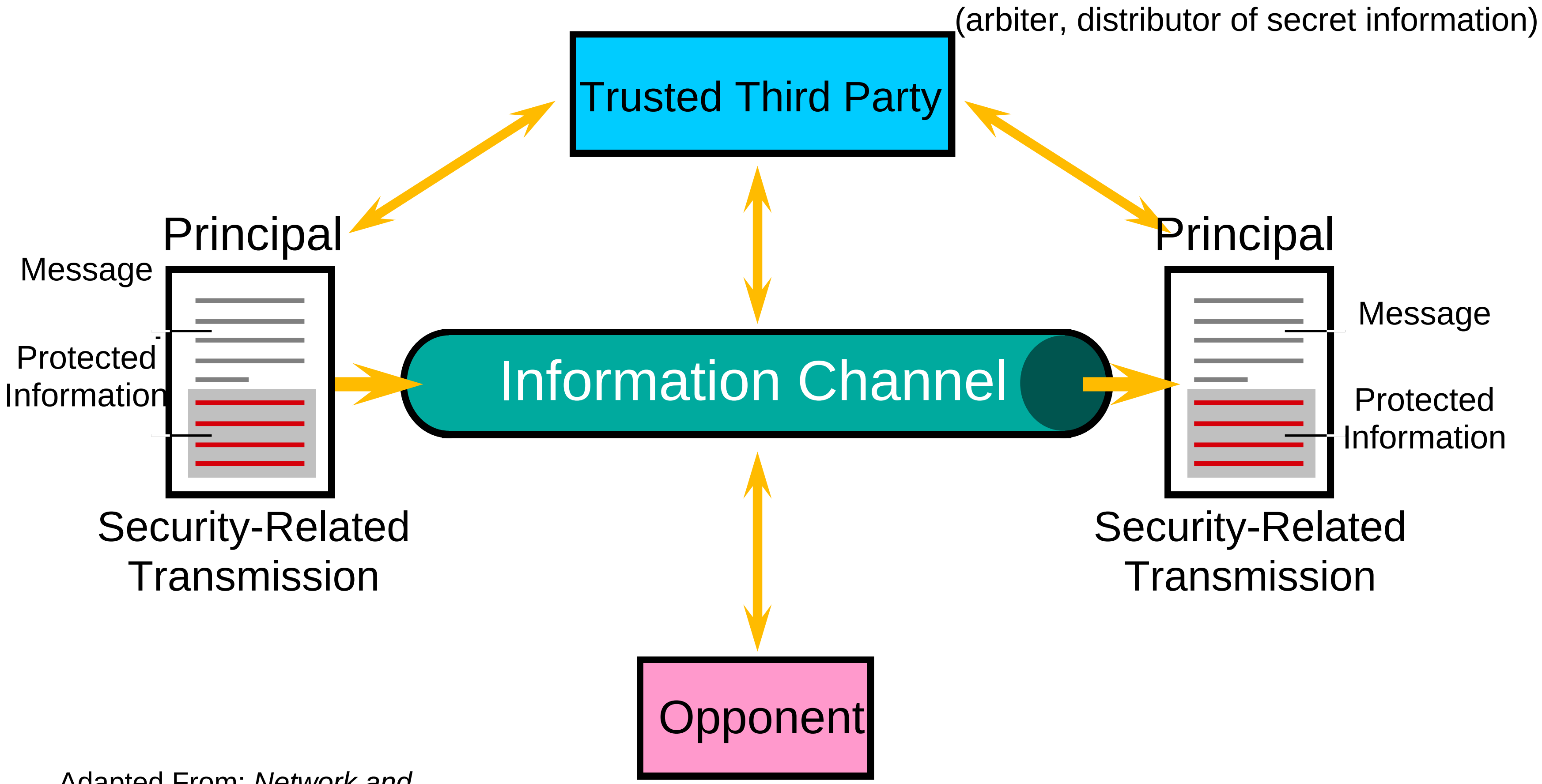


Alice

Bob

Eve

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...

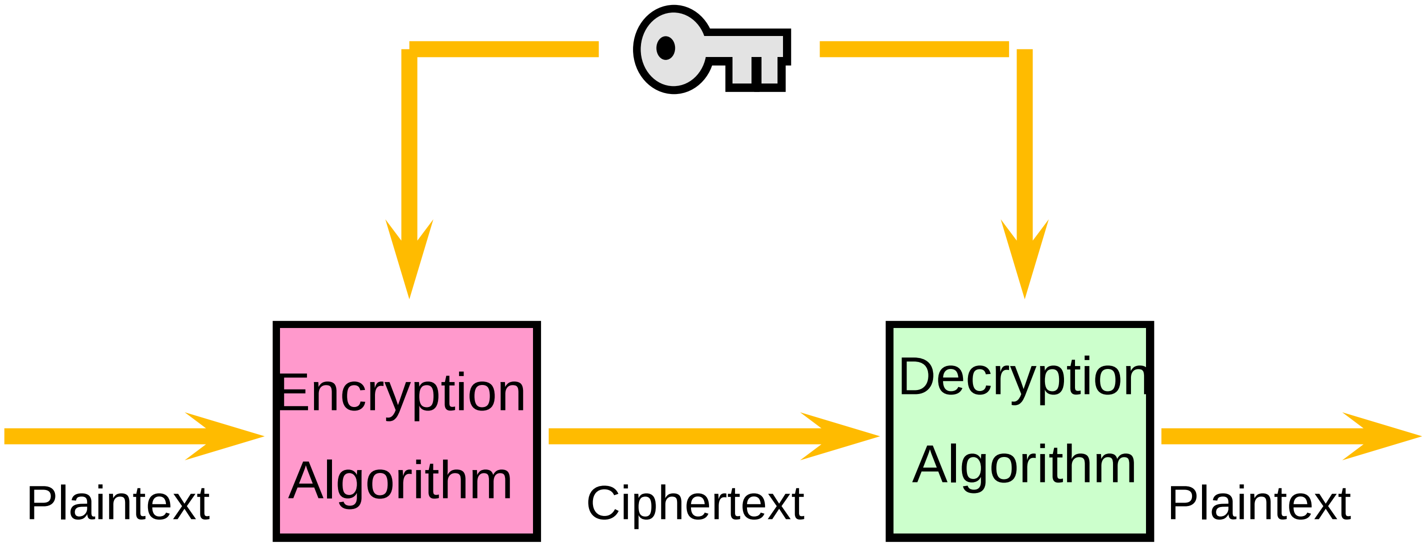
What is hashing?

- “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)

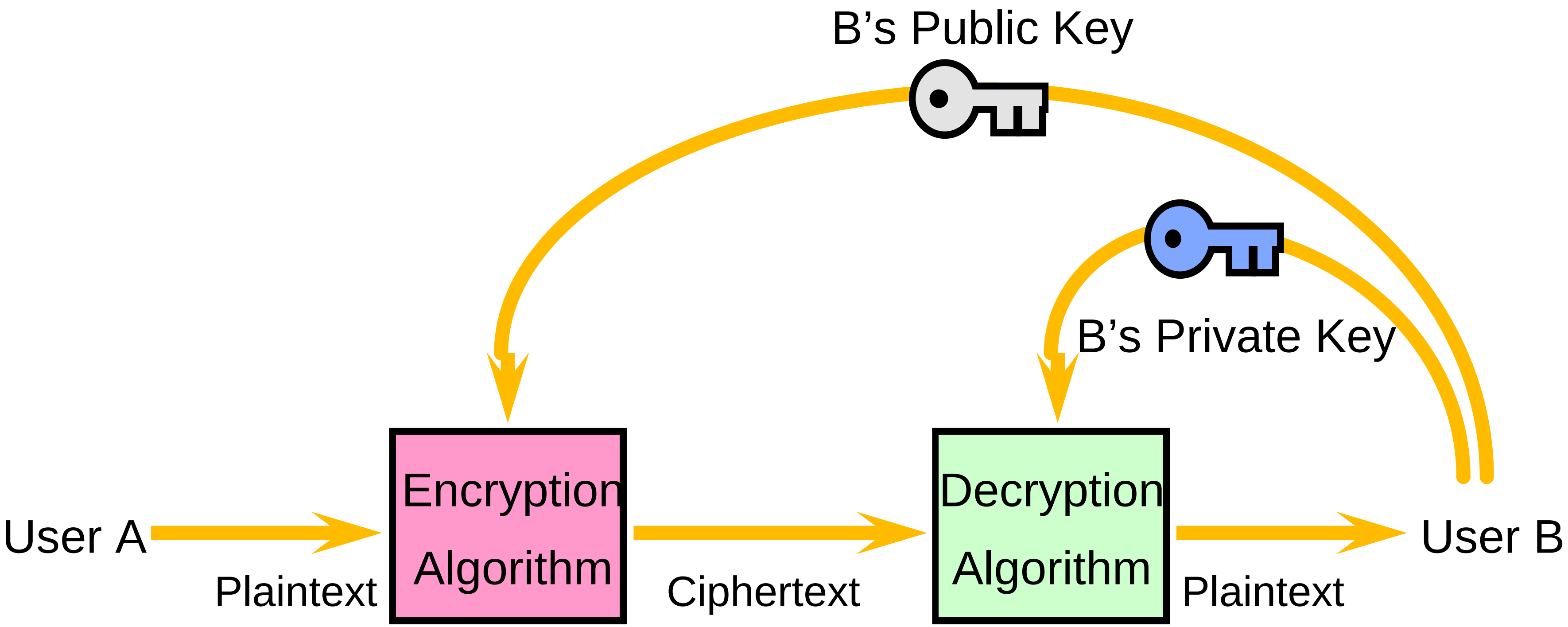
... It will be a blustery day in for Scotland with gales and showery rain in the north-east. Elsewhere in Scotland the showers will be more scattered at first with a few sunny spells, but outbreaks of rain will spread from the south-west this afternoon. Northern Ireland, Wales and England will also have 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



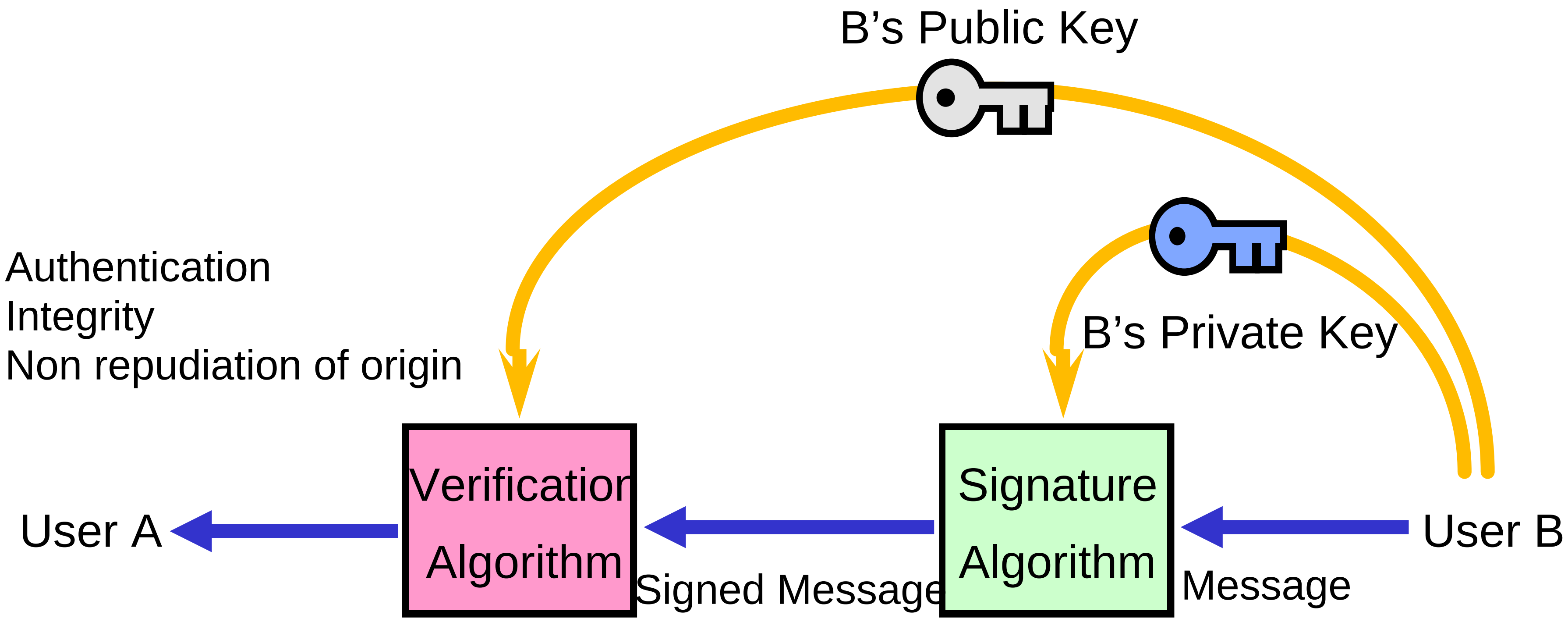
Adapted From: *Network and Internetwork Security* (Stallings)

Simplified Model of Public-Key Encryption



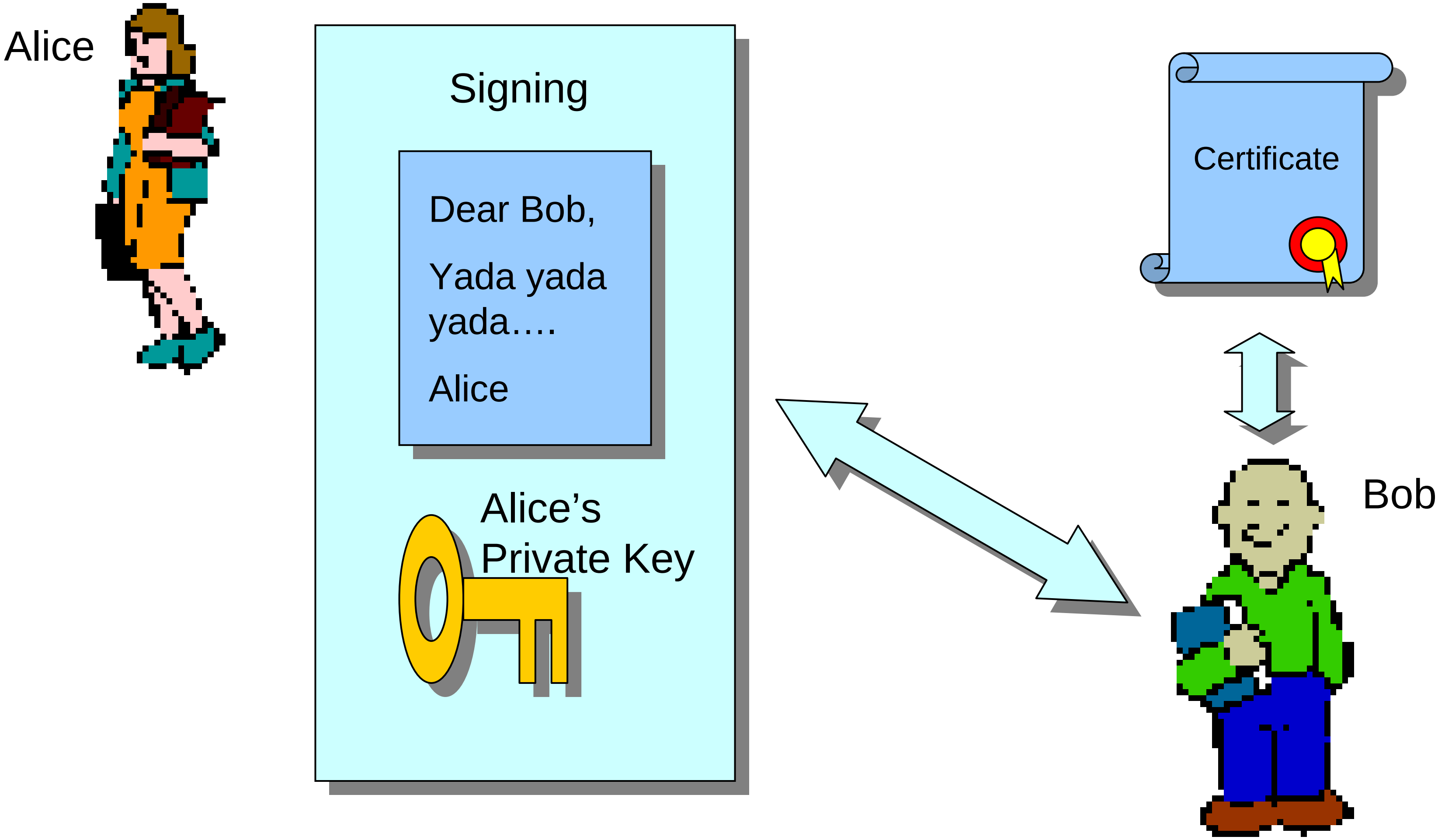
Adapted From: *Network and Internetwork Security* (Stallings)

Simplified Model of Public-Key Signatures



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

What are Digital Signatures?



Alice

Signing

Dear Bob,

Yada yada yada….

Alice

Alice’s Private Key

Certificate

Bob

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

- **Authentication**
  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.

Identification vs. Authentication

Determination of a person’s identity. (1:N)

“Positive authentication”

Hard to achieve

- Small user groups.
- Low accuracy.
- Exception: iris scan.

Verification of a person’s identity claim. (1:1)

Easier than identification.

User group size – accuracy!

Means of authentication	Access to a service
• something you know (password, PIN)	• Access by a person (process) that knows a secret.
• something you have (key, smartcard)	• Access by a person possessing a “key”.
• something you are - biometrics	• Access by a person with this characteristic.
• or combination of the above	

Something you know

+ Easy transport
+ Not a physical object
+ Easy & Fast control
+ Easy maintenance
+ (Low cost)

– Easy to copy after discovery

– Can be discovered without user’s knowledge

– Limited by human memory

– Can be forgotten

Something you have

+ Hard to copy
+ Loss easy to discover
+ The object itself can process information

– Need of reader

– User is not recognized without the object

– The object must be complicated so that it is hard to copy

– Can break down, this often not detected easily

Something you are

+ Is part of a person
+ Cannot be lost

– Accuracy
– Protests/resistance of users
– Hard to measure
– Limited number of object to use ☺

Combine!

- Multifactor authentication
  - Something you know
  - Something you have
  - Something you are
- ATM/Banking card – card + PIN
- Spoken passphrase – passprase + speaker recogn.
- Really smart smartcard – card + PIN + fingerprint

Passwords

- Group passwords common to all users (in a group) of a system
- Passwords unique to individual users
- Non-unique passwords confirming identity
- One-time passwords

Don’t store passwords in clear text!

- Salting technique
  - – userID, salt, hash(password, salt)
  - – Effective password
    - Longer
    - Not a common word/combination
  - – Two users with the same password have different entries in the password database.

Passwords

Human memory vs. security

(short easy-to-guess string vs. long complicated string)

- Dictionary attack
  - All combinations of up to 5-8 characters.
  - Common words and user-related values.

  - Usual success rate 20-40%

Choice of passwords – problems

- Easy to remember for the user and hard to guess for anyone else

- Requested change (password “circulation”)
- Password selection without user input ☹
- Same password over more systems

Choice of passwords – suggestions

- Password (choice) quality control!!!
- Special characters, Shift, substitutions (phonetic, mnemonic)
- Use phrases: *Early One Morning With Time To Kill* (☺ Sting) – EY1ghe2KL

- Enforce your password security policy through some mechanism!!!

Banks – card & PIN

- Personal Identification Number
  - Every combination with same probability
  - Not discarding “easy” combinations
  - Not only 4, but up to 8 (6) digits
  - Markus Kuhn – Cambridge (UK) – ref. later
- Distribution of card, PIN
  - Both via different routes (or instances)
  - Personal retrieval (of at least one)
  - PIN of own choice

Suggested (not required) readings

- M. Kuhn: *Probability Theory for Pickpockets – ec-PIN Guessing* **`http://www.cl.cam.ac.uk/~mgk25/ec-pin-prob.pdf`**
- J. Yan et al.: *The memorability and security of passwords – some empirical results*, University of Cambridge Computer Laboratory Technical Report No. 500 **`http://www.cl.cam.ac.uk/TechReports/`**

Tokens

- Keys
- Magnetic cards (3-track strip ~ 250 B)
  - Easy to copy
    - Shifting tracks of limited use
    - Individual characteristics of tracks can be of some use
  - PIN manipulation also easy
- Bank cards – with signature, possibly PIN
  - *Customer Not Present* transactions problematic

Smartcards

- Smartcard vs. Chipcard
- Can store (some even work with) a crypto key
- Cash-loading (anonymous vs. loss-recoverable)
- GSM – authentication key; PIN-PUK
- Implementation in bank cards
  - Compatibility – users, retailers(!) (VISA – 2007)
  - Potentially can be used with biometrics

Authentication calculators

- Challenge-response based
  - Response = *f(secret key, challenge)*
- Time-based (SecurID)
  - Server takes care of time-frame shifts

- Transfer – manual vs. automatic
- PIN – standard and emergency

Biometrics

- PIN/password either matches (at 100%) or not

- Biometrics rarely match at 100% (often taken as a fake/attack).

- Threshold-based decision introduces the rates of false acceptance and rejection

- **Verification** (of identity) - 1:1 match)

- **Identification** - 1:N search for the best match

Biometrics – major issues

- Biometrics are very sensitive
- Biometrics are not secrets
- Copying: neither trivial nor hard
- New attack countermeasures are followed by newer attacks

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*

Course 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

- Study of… a virus, a particular security solution/system, crypto algorithm…
- Security of … JavaCard 3.0, smartcard X…
- New… firewall, IDS, mobile security app, malware trend…
- **Focus (don’t go for broad topic/area)!**
- Mail me, with Subject: PA018 – term project
- **Deadline for proposal *and approval* – Feb 28!!!**

Questions, comments, suggestions…???

Go ahead!

☺