Information & Communication Security (SS 15)

Questions and answers – Exam preparation

J. Serna-Olvera, W.B. Tesfay, and F. Veseli
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

mobile business

What is the difference between Password Spoofing and Phishing?

Password Spoofing

- Identification and authentication through username and password only provide *unilateral authentication*.
- Does the user know who has received the password? -> No
- The user has no guarantees about the identity of the party at the other end of the line.

Password Spoofing

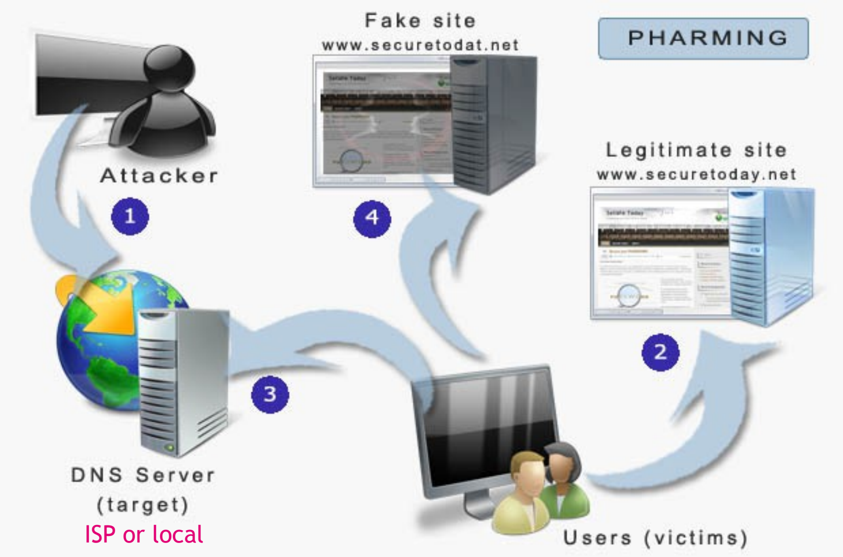
- The attacker runs a program that presents a fake login screen.
- An unsuspecting user tries to login at that terminal.
- The victim is asked for username and password.
- These are then stored by the attacker.
- Login is aborted with a (fake) error message and the spoofing program terminates.
- Often, the user is then redirected to the real login screen.

Spoofing

- Spoofing: falsification of information, an attack in which the client is given false information that leads the client to request a session with the hacker’s computer rather than the real server.
- Examples: MAC spoofing, DNS spoofing, proxy manipulation

Example: Pharming

- When users ask for an IP address to match a URL, a wrong one is provided.
- Attack against DNS server or user‘s PC.



Source: http://www.securetoday.net/

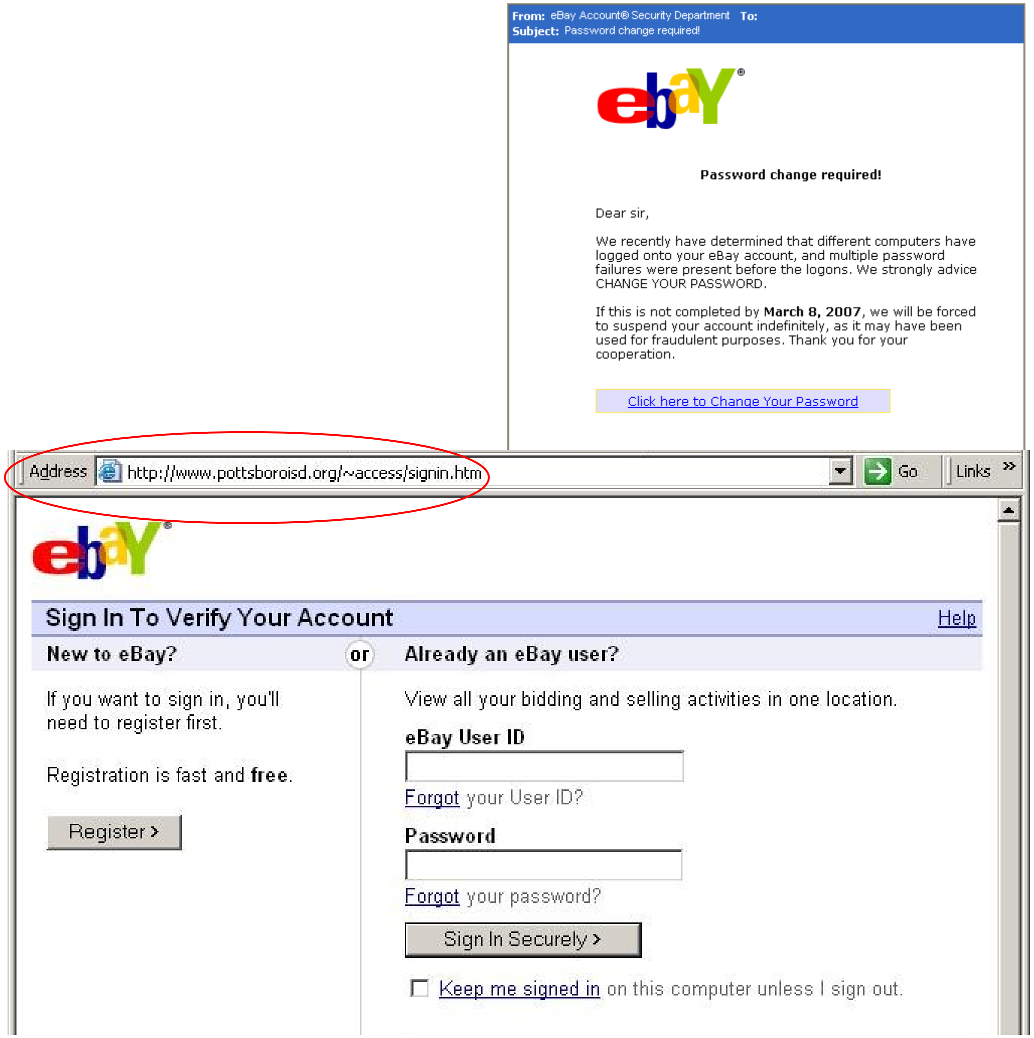
- When users try to access the attacked website they are redirected to the fake site

Example: Phishing

Scam e-mail

Link to fake login form

Fake address **visible** in URL



From: eBay Account® Security Department **To:**
Subject: Password change required!

Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD.

If this is not completed by **March 8, 2007**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

Click here to Change Your Password

Address http://www.pottsboroisd.org/~access/signin.htm

Sign In To Verify Your Account Help

New to eBay? or **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

Register >

View all your bidding and selling activities in one location.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

Sign In Securely >

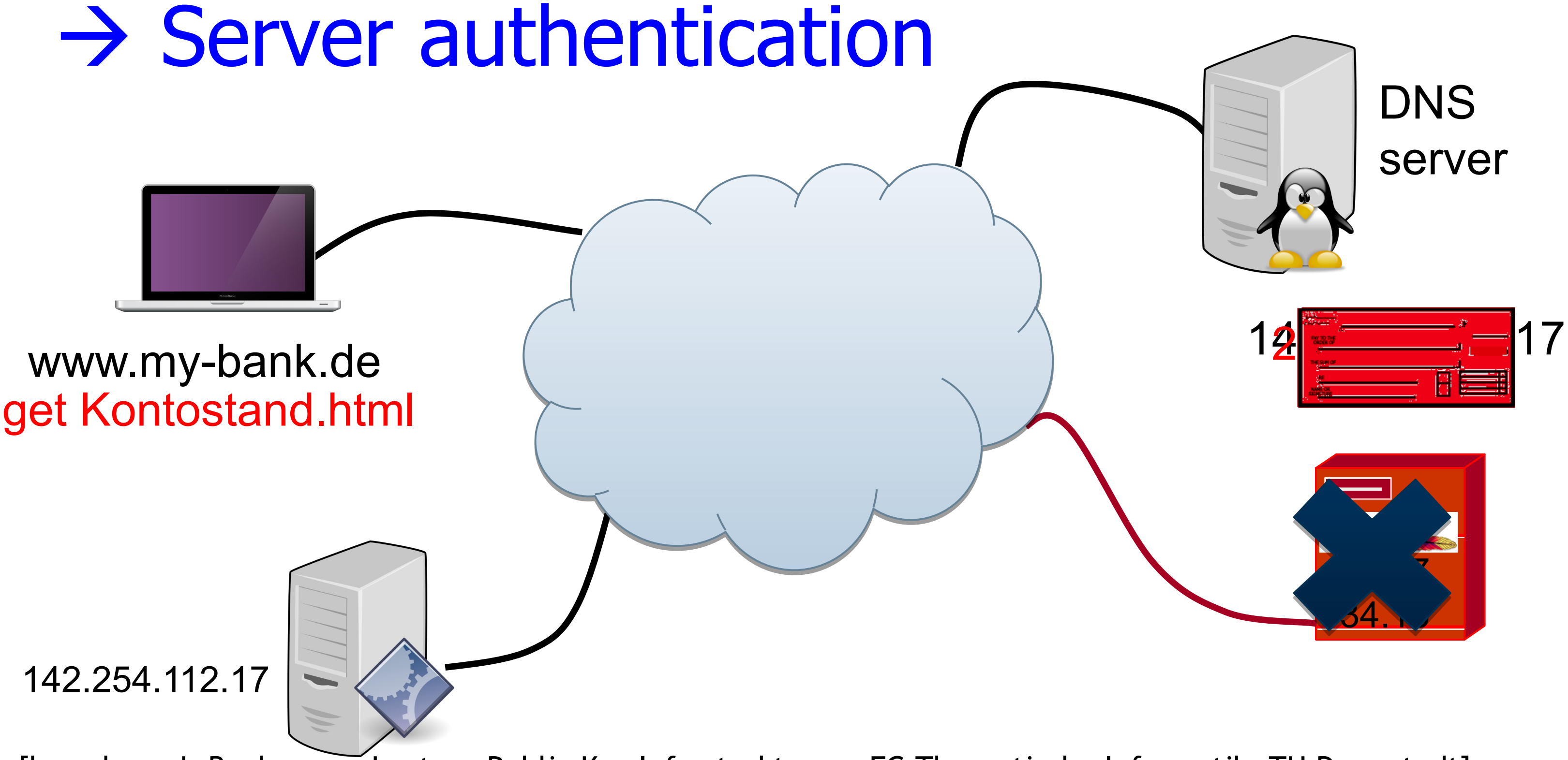
□ Keep me signed in on this computer unless I sign out.

Can you explain the DNS and HTTP spoofing?

DNS spoofing

Possible attacks:

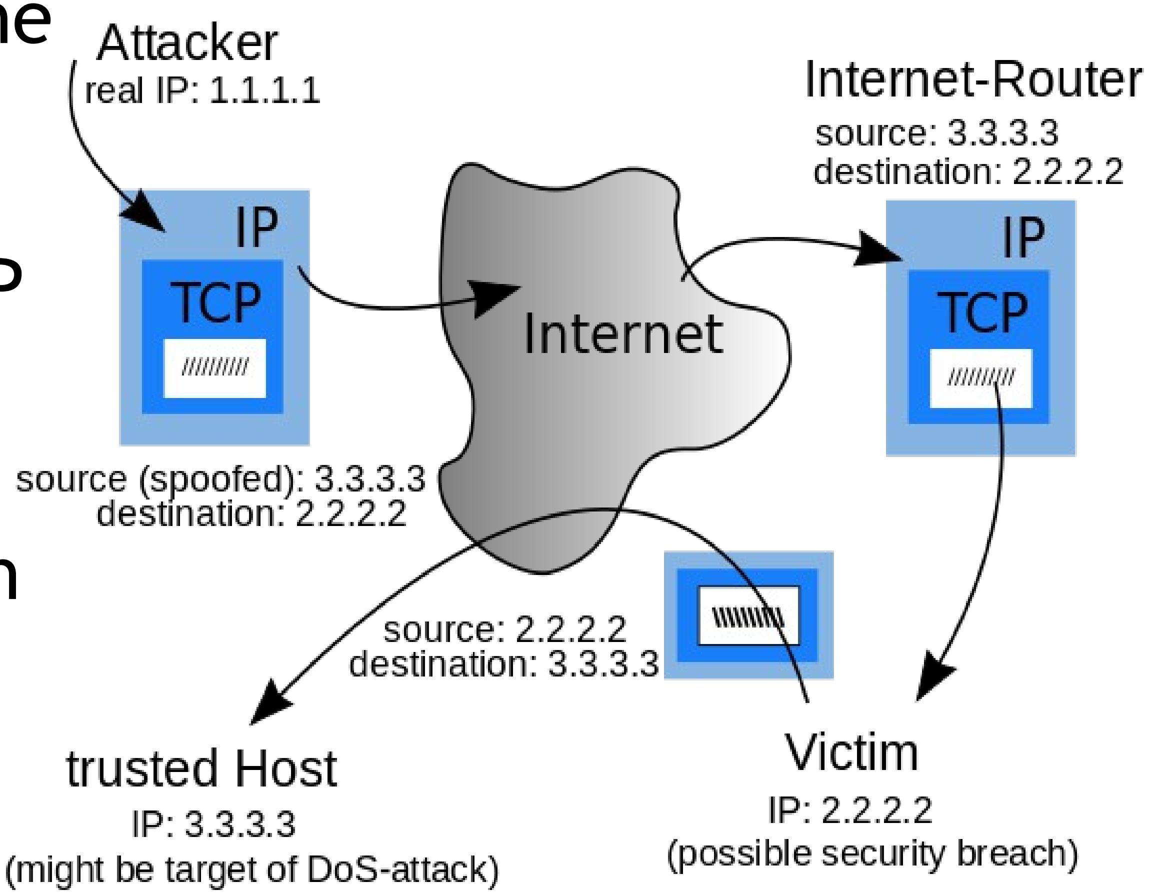
1. Compromise of DNS (DNS spoofing)
   → Server authentication



[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

IP-Spoofing

- IP spoofing is the creation of IP packets with a forged source IP address.
- Attacker sends IP- packets with a faked sender address.



What is the difference between known-plaintext attack and chosen-plaintext attack?

Attacks

- In a *ciphertext only* attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.
- In a *known plaintext* attack, the adversary has the plaintext and the ciphertext that was enciphered. Her goal is to find the key that was used.
- In a *chosen plaintext* attack, the adversary may ask that specific plaintexts be enciphered. She is given the corresponding ciphertexts. Her goal is to find the key that was used.

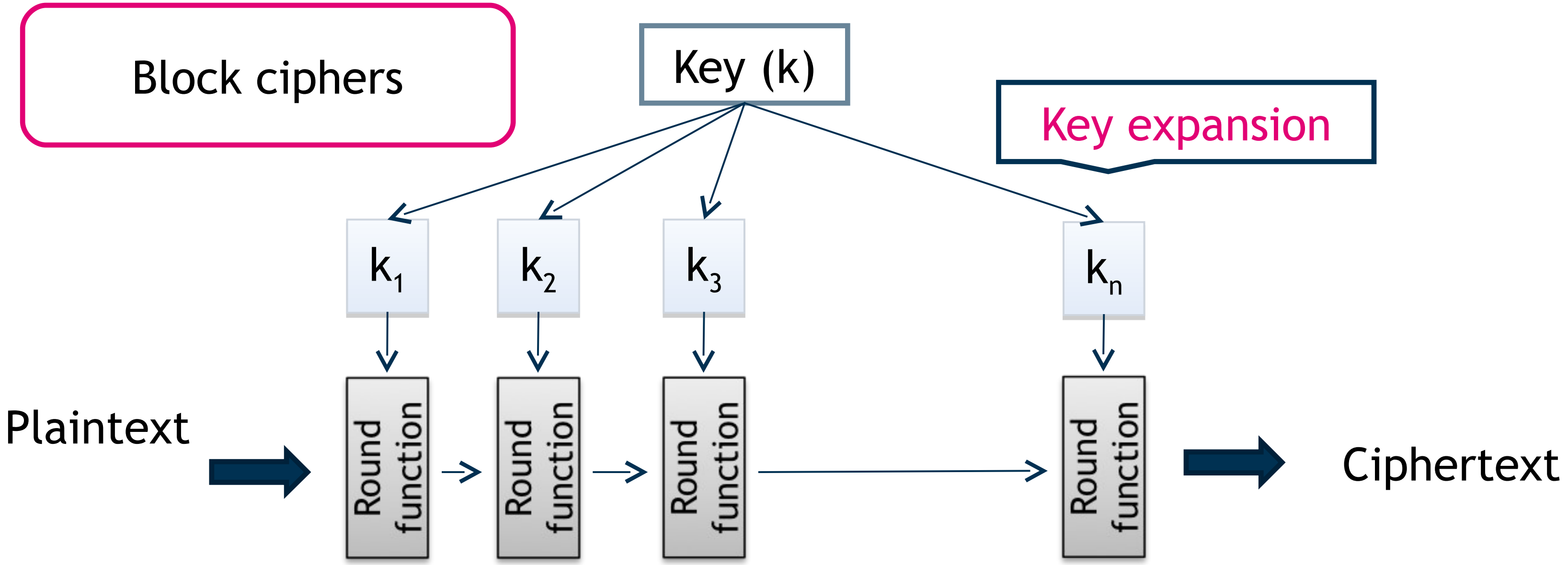
[Bi2005]

What do we need to know about AES?

AES Encryption - Overview

- AES encryption
  - has a variable **number of rounds (10, 12, 14)**
  - depending on **key size (128-bit, 192-bit, 256-bit)**.
- To encipher a block of data in AES
  - Initialize (key schedule…)
    - Stretch key data
    - Initialization Round
  - Then several rounds of encryption
    - Shifting and mixing bits
  - Finally, some postprocessing
    - perform a round with the last step omitted

Advanced Encryption Standard



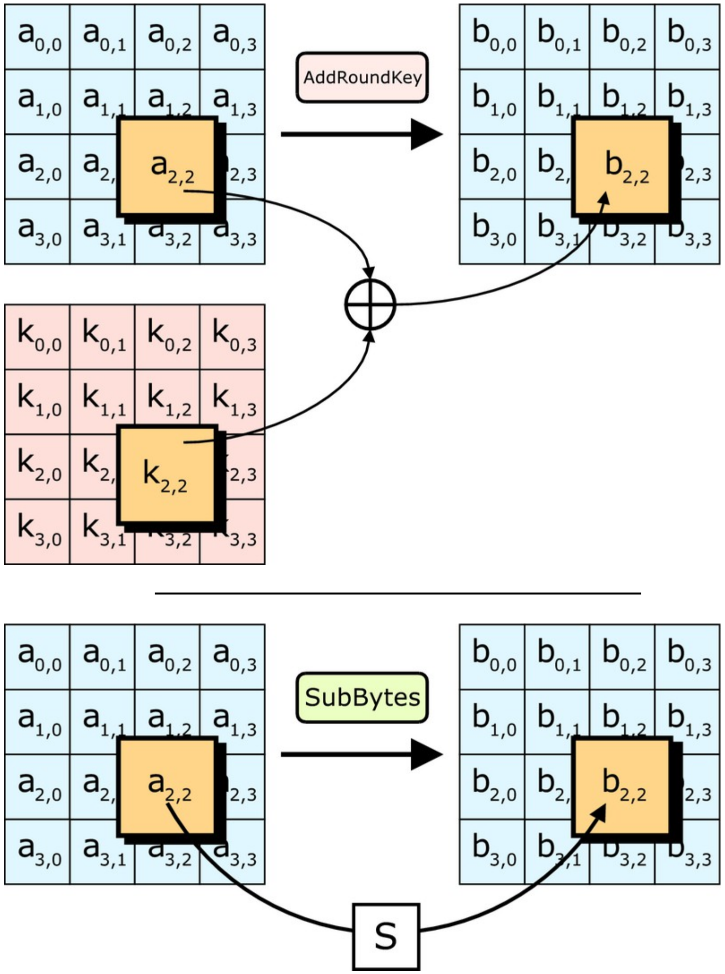
- This new cipher is called Advanced Encryption Standard (AES).
- AES has been approved for Secret or even Top Secret information by the NSA.

[Bi2005]

Encryption Round (1)

AES

- AddRoundKey
  - XOR (mix bits of) current state a and round key
  - Round key k derived using key schedule
- SubBytes
  - Substitution using a lookup table (S-Box)

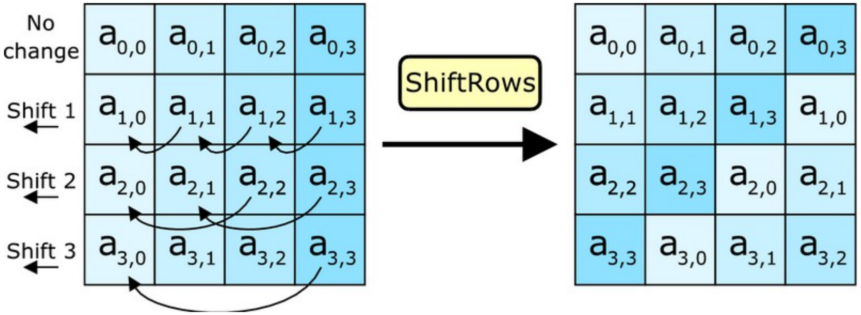


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$
SubBytes
S

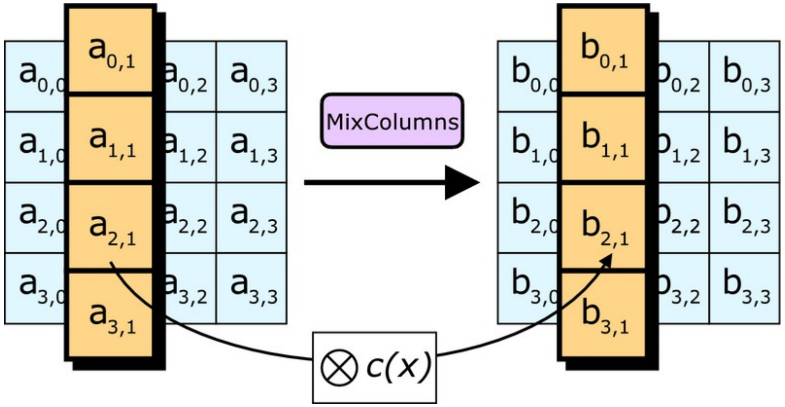
Encryption Round (2)

AES

- ShiftRows
  - Shift each row by row index
- MixColumns
  - 4 key bytes combined into each column using polynomial multiplication modulo 2^8 [in $GF(2^8)$]



No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$



$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

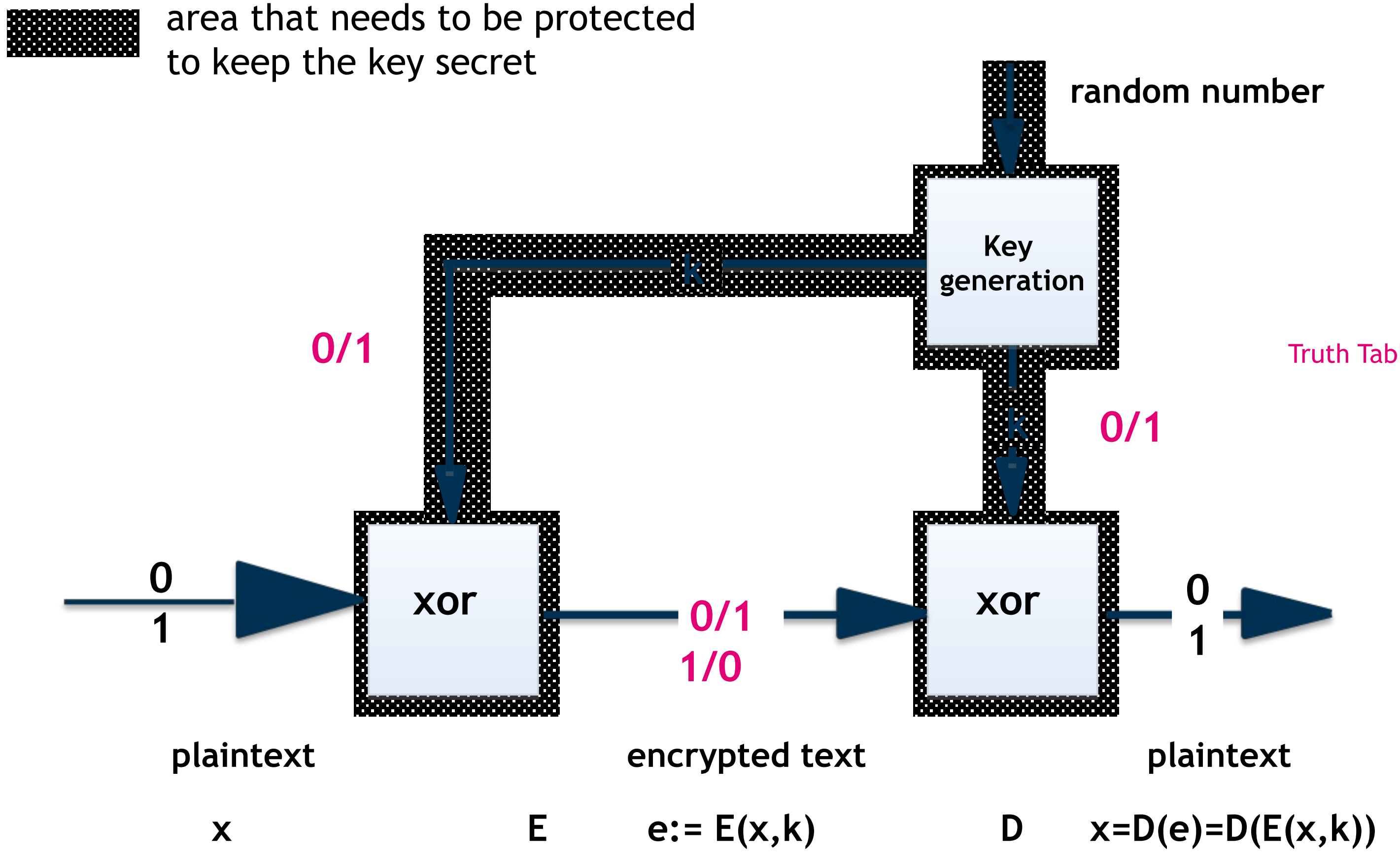
mobile business

Why do we need the XOR and how it works?

One Time Pad

- Invented by Gilbert Vernam
- The one-time pad is basically a Vigenére cipher.
- The length of the key is as long as the length of the plaintext.
- Therefore, there are no periodic reoccurrences.
- The key is randomly chosen and only used once.
- Every key has the same probability.

Example One Time Pad



X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

[based on Federrath and Pfitzmann 1997]

Example

PT=	0	1	1	0
k=	1	0	1	1

X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

a=	1	1	1	1
b=	1	0	1	1
c=	1	1	0	1

mobile business

Can you explain Hybrid Cryptographic Systems?

Performance of Public Key Algorithms

Algorithm	Performance*	Performance compared to Symmetric encryption (AES)
RSA (1024 bits)	6.6 s	Factor 100 slower
RSA (2048 bits)	11.8 s	Factor 180 slower

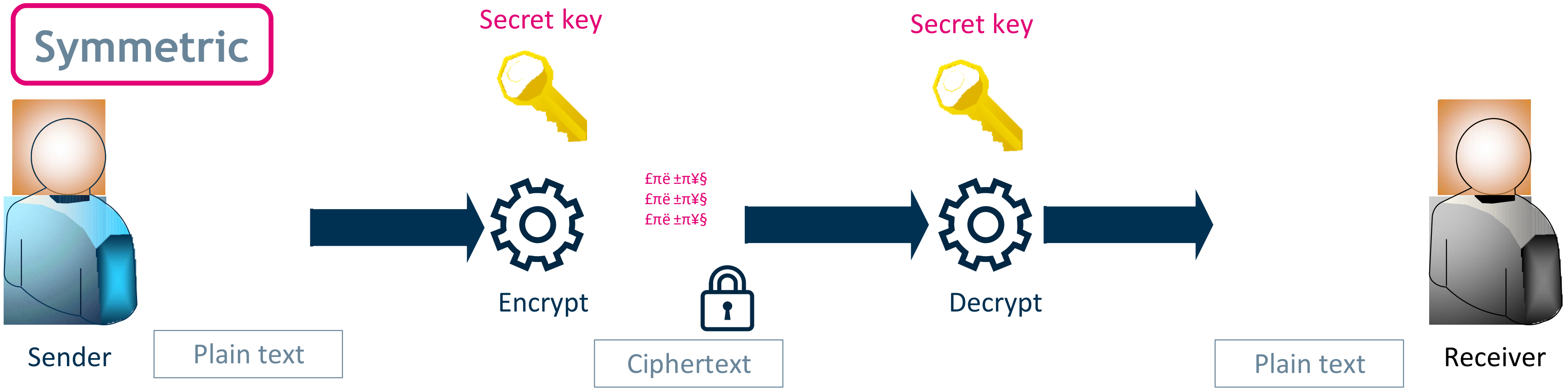
Disadvantage: Complex operations with very big numbers

[**Algorithms are very slow.**

* Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider (Java)

[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Cryptographic Systems (II)



Symmetric

Secret key

Secret key

Sender

Plain text

Encrypt

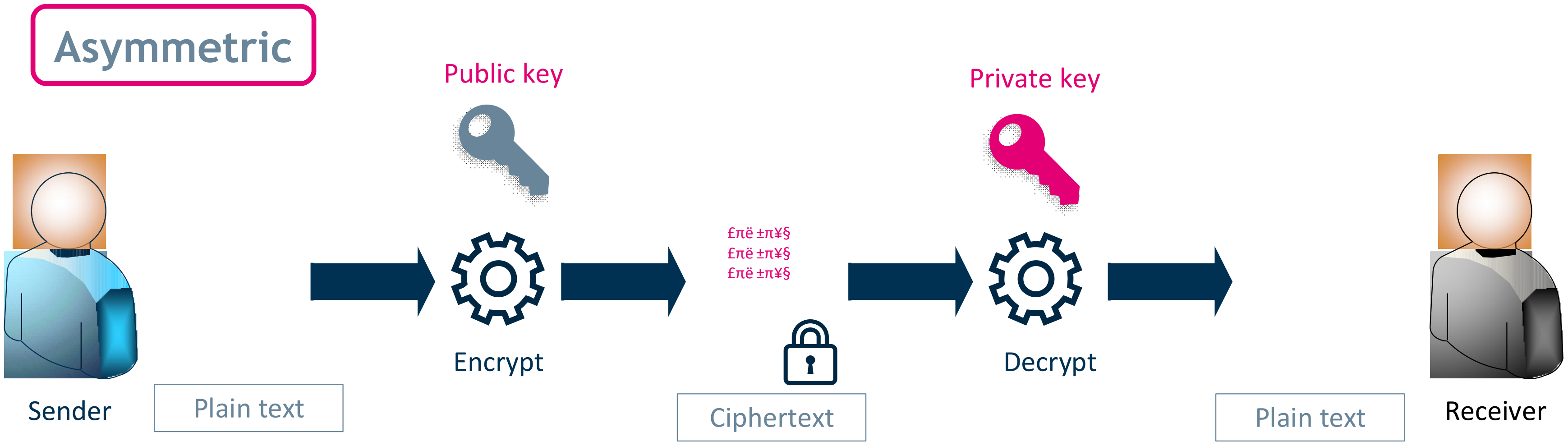
£πë ±π¥§
£πë ±π¥§
£πë ±π¥§

Ciphertext

Decrypt

Plain text

Receiver



Asymmetric

Public key

Private key

Sender

Plain text

Encrypt

£πë ±π¥§
£πë ±π¥§
£πë ±π¥§

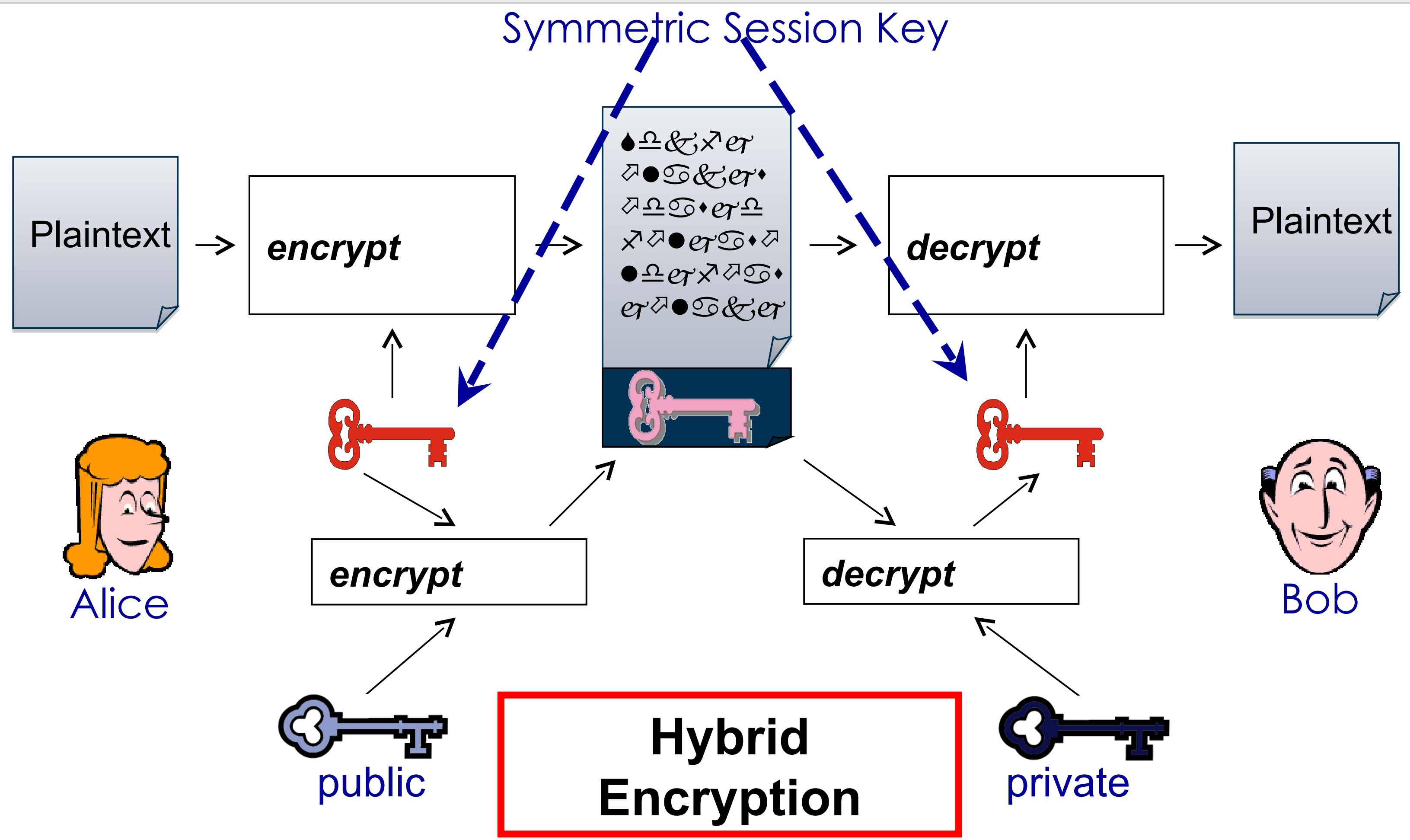
Ciphertext

Decrypt

Plain text

Receiver

Solution: Hybrid Systems



Symmetric Session Key

Plaintext → *encrypt* → → *decrypt* → Plaintext

encrypt

decrypt

Alice

Bob

public

private

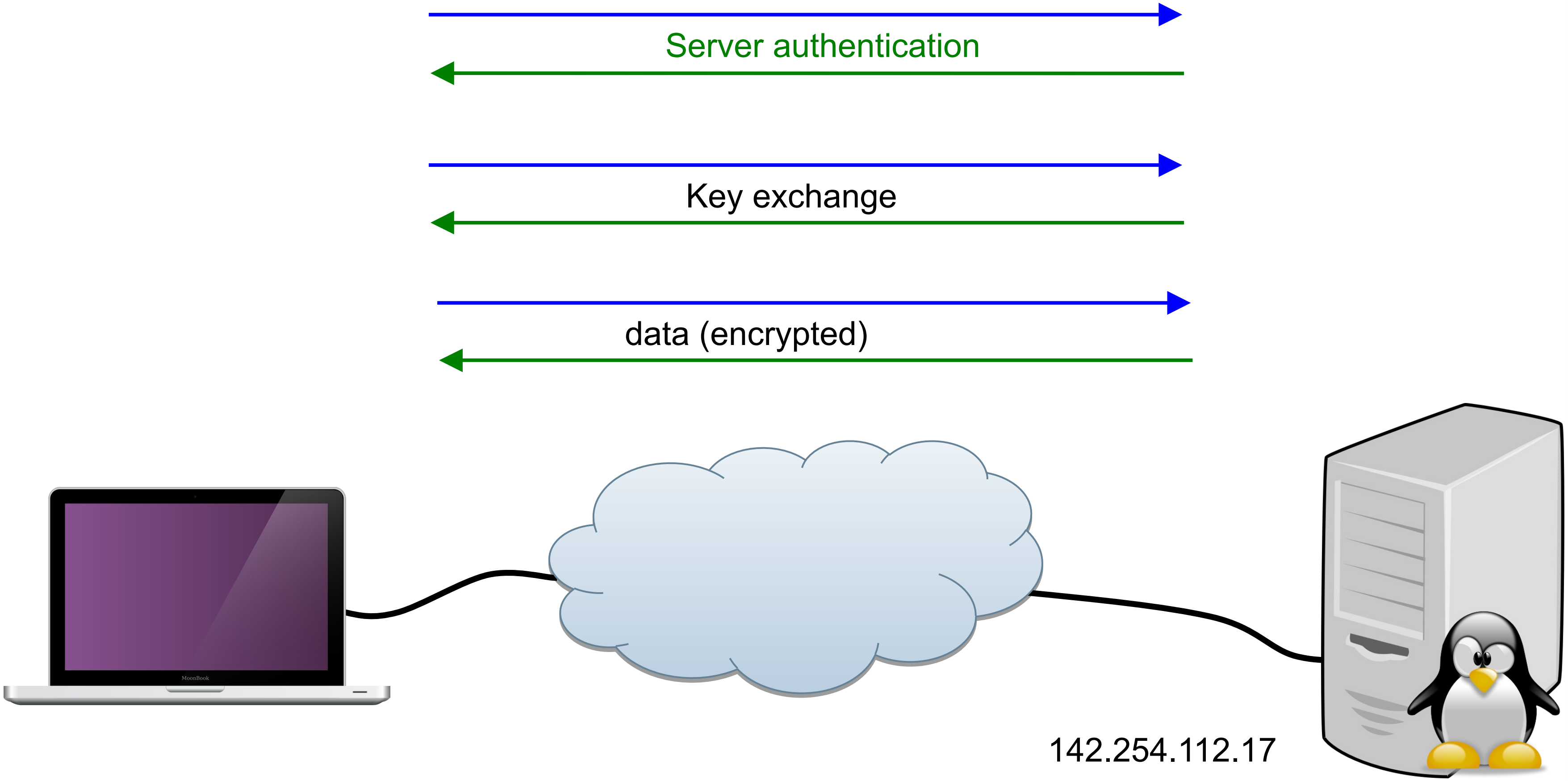
Hybrid Encryption

[based on: J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Can you explain SSL/TLS?

SSL/TLS

SSL/TLS (simplified):



Hello!

Server authentication

Key exchange

data (encrypted)

142.254.112.17

[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

SSL/TLS

SSL/TLS:

- Server- and client-authentication
- Key exchange for symmetric encryption
- MACs to secure integrity

Security Goal	http	https (SSL/TLS)
Authenticity	✗	✓ (mostly server only)
Non-Repudiation	✗	✗
Confidentiality	✗	✓
Integrity	✗	✓
Date documentation	✗	✗

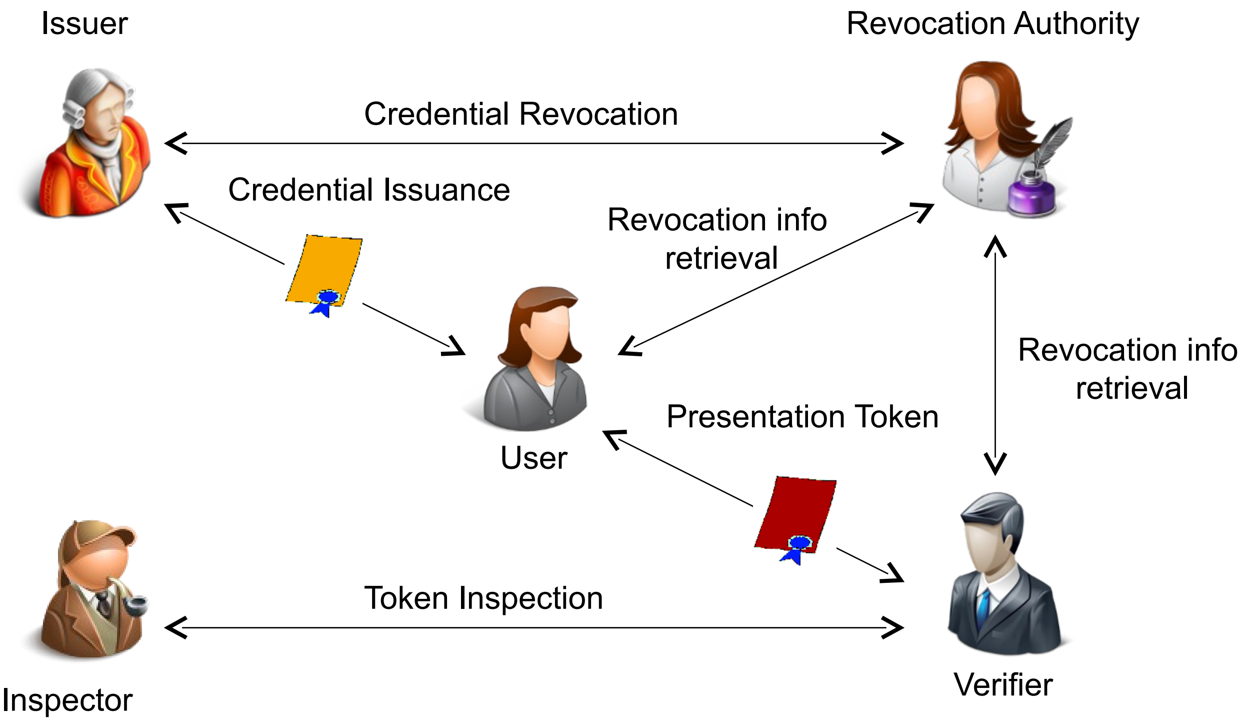
Based on [J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Authentication

Lecture 2 Slide 47+48 ABC4 Trust (same Lecture 8, Slide 36/37)

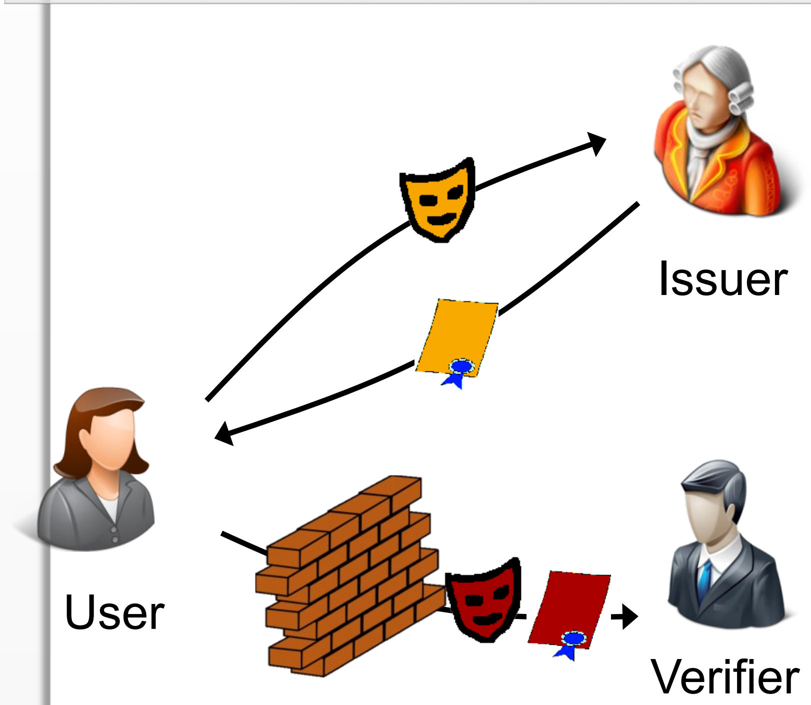
ABC4Trust architecture

Interactions and Entities



Existing Privacy-ABC Technologies

Zero-Knowledge Proofs

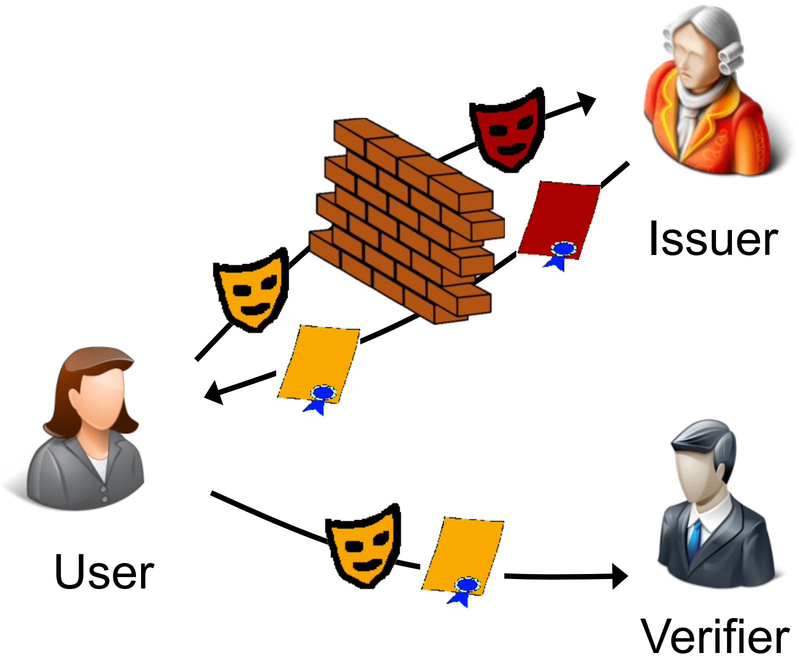


Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya

Strong RSA, pairings (LMRS, q-SDH)

Blind Signatures



U-Prove

Chaum, Brands et al.

Discrete Logs, RSA,…

Privacy protection

1. Can you explain the Mixes and Onion Routing again?
2. Lecture 8 Slide 20 Mixes and Slide 24-31 Tor Network.

Privacy-preserving Communication Systems

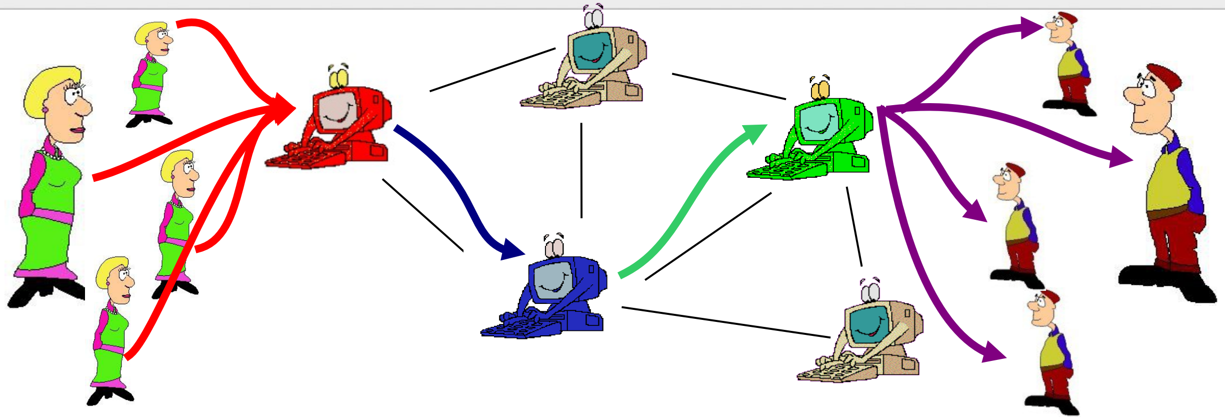
- Mixmaster – Anonymous Remailer

  http://mixmaster.sourceforge.net

- Onion Routing: Tor Network

  http://tor.eff.org/

Mixes and Onion Routing

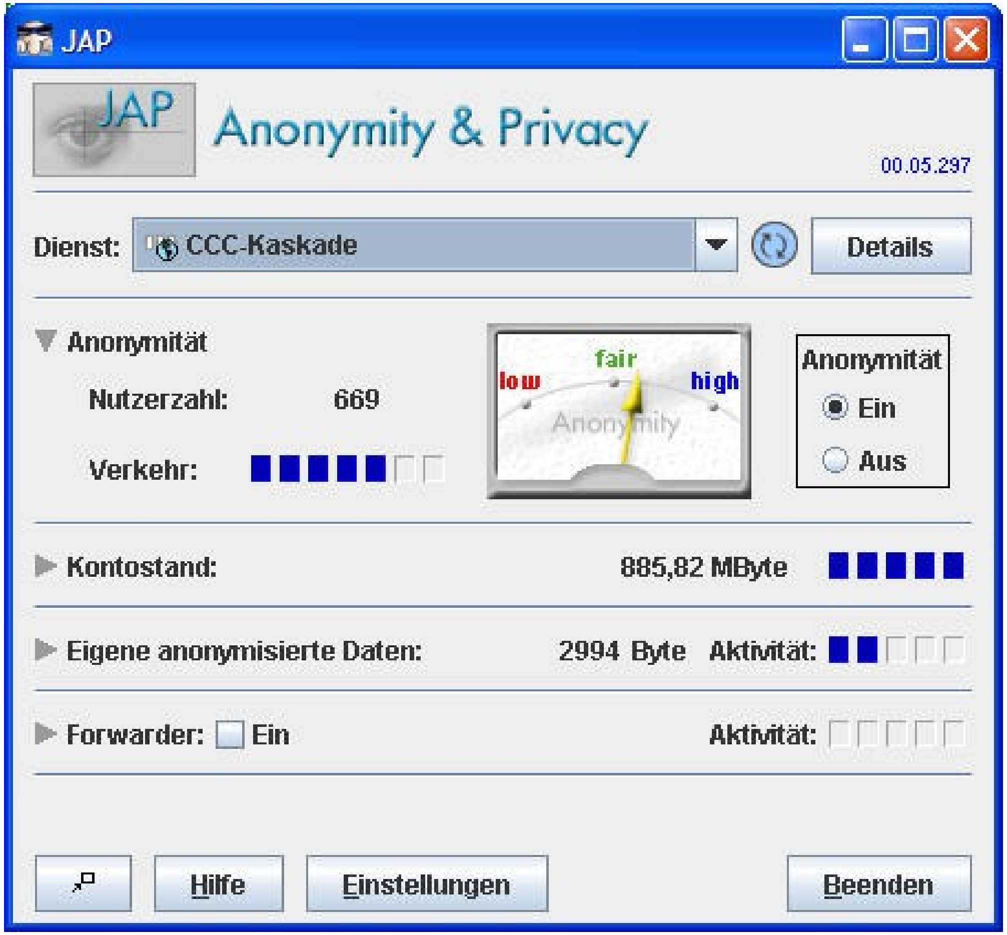


- *Communication is anonymised by multiple mix servers, also called onion routers.*
    - *Both onion routing and JAP are based on the same Mix concept.*

Java Anonymity Proxy (JAP)

- Users can choose between multiple mix-cascades
- Number of active users is a heuristic for level of anonymity achieved
- Current version does not achieve security against a global attacker but can protect against local attackers
  - your boss
  - your provider
  - operator of a mix

http://anon.inf.tu-dresden.de



JAP

JAP Anonymity & Privacy

00.05.297

Dienst: CCC-Kaskade

Anonymität

Nutzerzahl: 669

Verkehr: ■■■■■□□

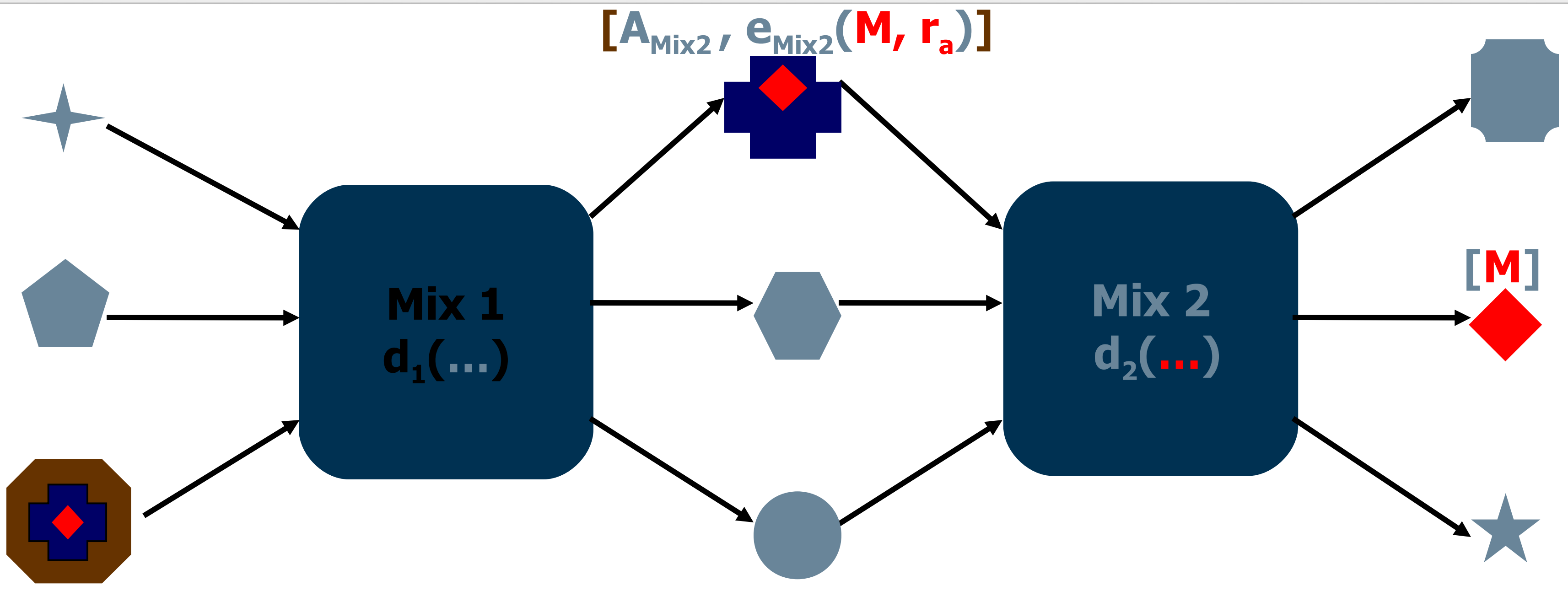
Anonymität ● Ein ○ Aus

Kontostand: 885,82 MByte ■■■■■

Eigene anonymisierte Daten: 2994 Byte Aktivität: ■■□□□

Forwarder: □ Ein Aktivität: □□□□□

Mixes



$[A_{Mix2}, e_{Mix2}(M, r_a)]$

$[A_{Mix1}, e_{Mix1}(A_{Mix2}, e_{Mix2}(M, r_a), r_b)]$

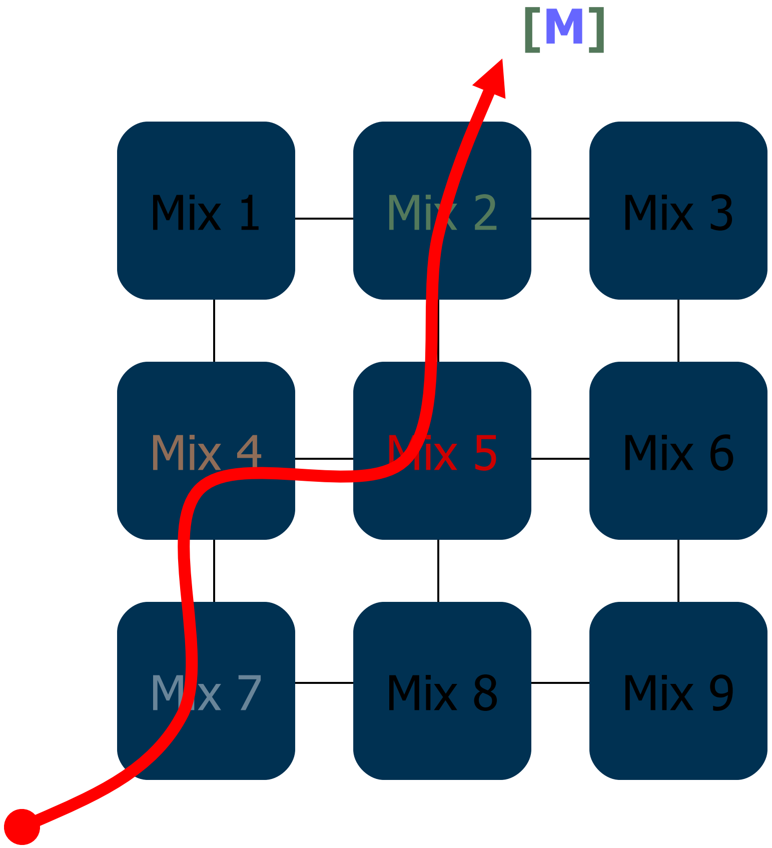
- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure [Chaum1981]

Symbols:

A	address
e()	encryption function
d()	decryption function
M	core message
r	random value
[]	message boundary

Mix Network

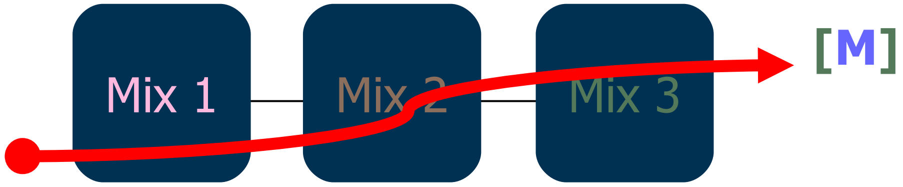
- Choose the way of your message through the mixes!
- Protection guaranteed as long as one chosen mix withstands attacks.
- Free path results in additional confusion, but smaller anonymity set.



$$[A_{Mix7}, e_{Mix7}(A_{Mix4}, e_{Mix4}(A_{Mix5}, e_{Mix5}(A_{Mix2}, e_{Mix2}(M, r_a), r_b), r_c), r_d)]$$

Mix Cascade

$[e_{Mix1}(e_{Mix2}(e_{Mix3}(M, r_a), r_b), r_c)]$



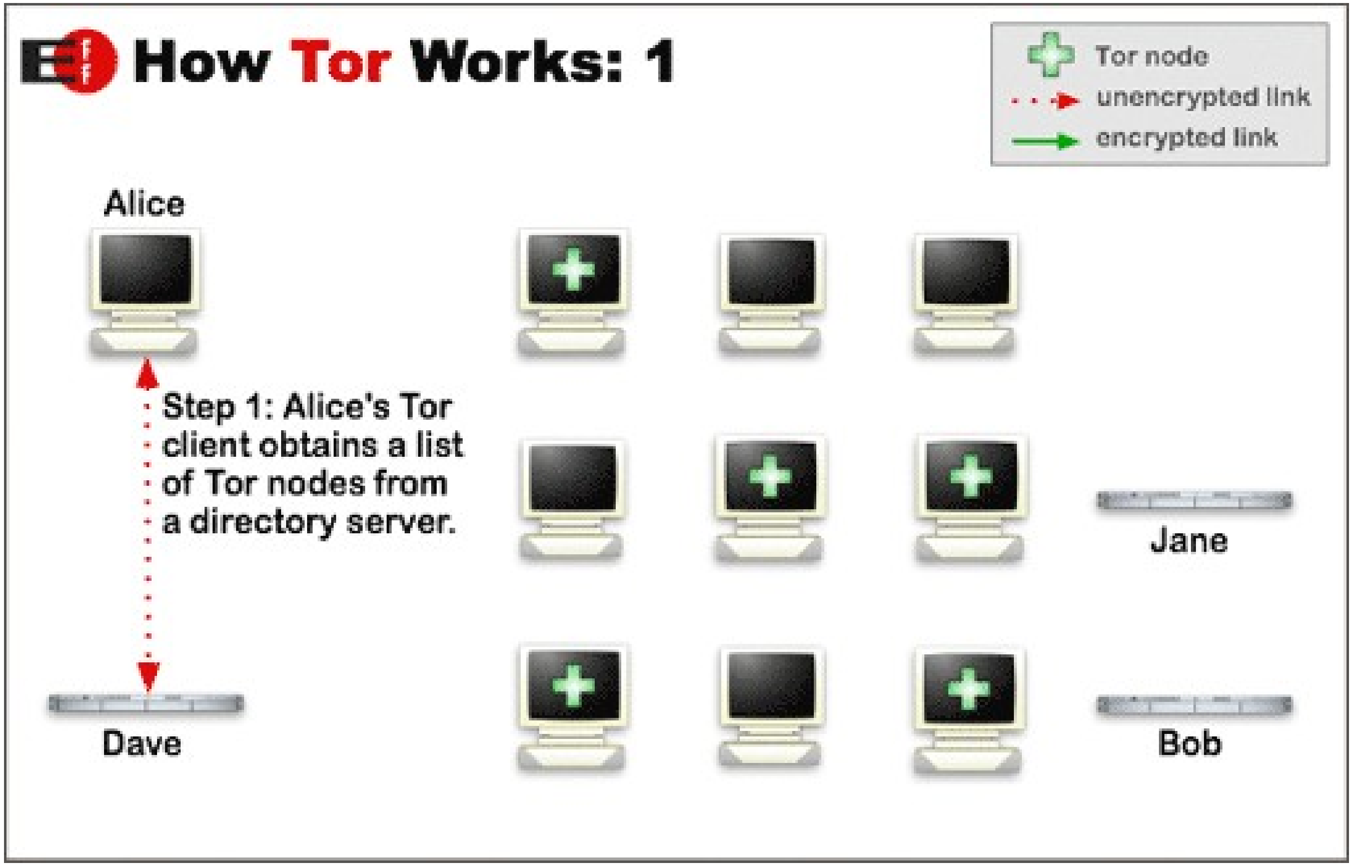
- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

Tor Network

- Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet
- Distributed anonymous network
- Tor allows users to change circuits during sessions
  - ➢ Aims to minimize linkability of actions
- May be affected by the data retention directive (as well as JAP)
  - ➢ Anonymity and data logs?

[Europe2006]

How Tor Works I

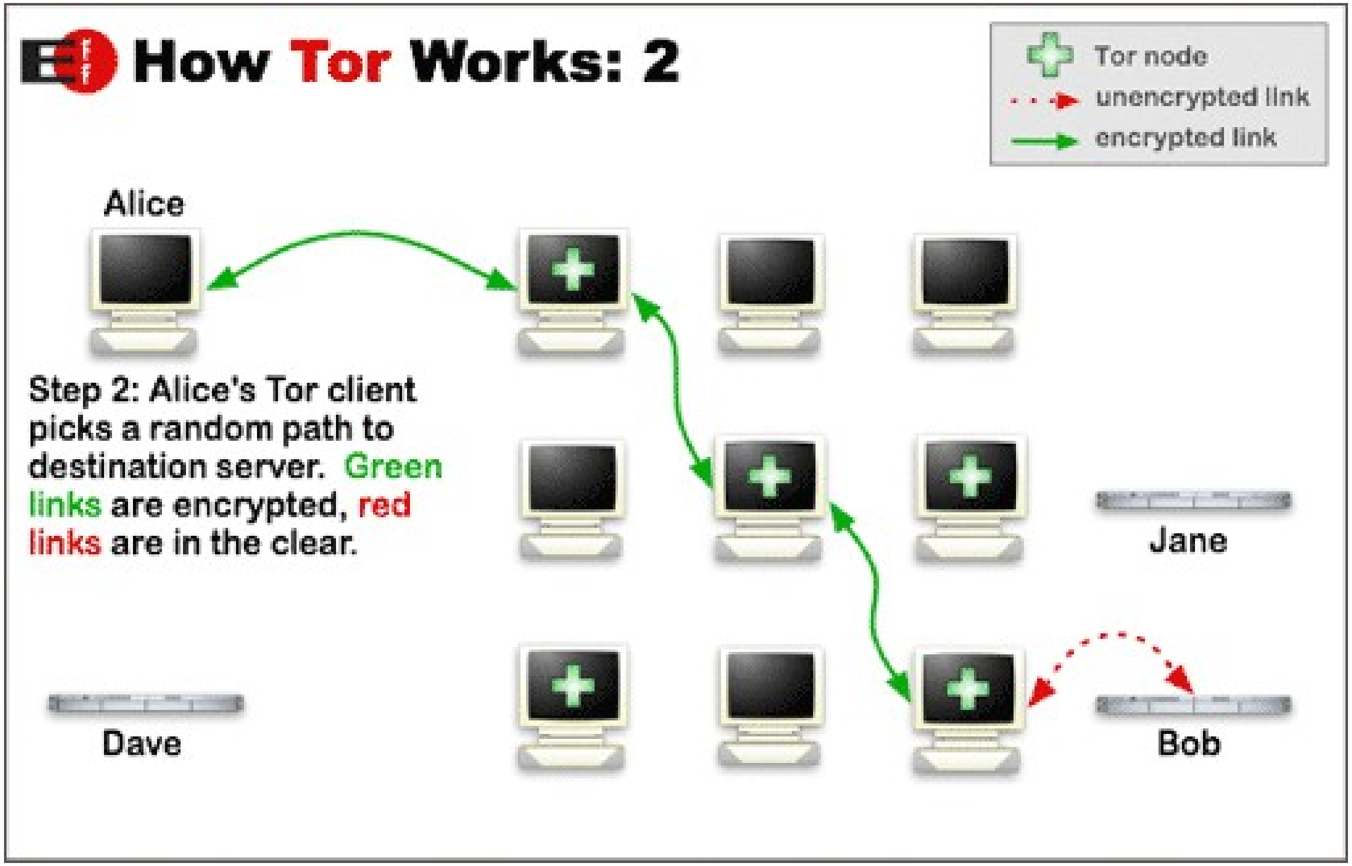


How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

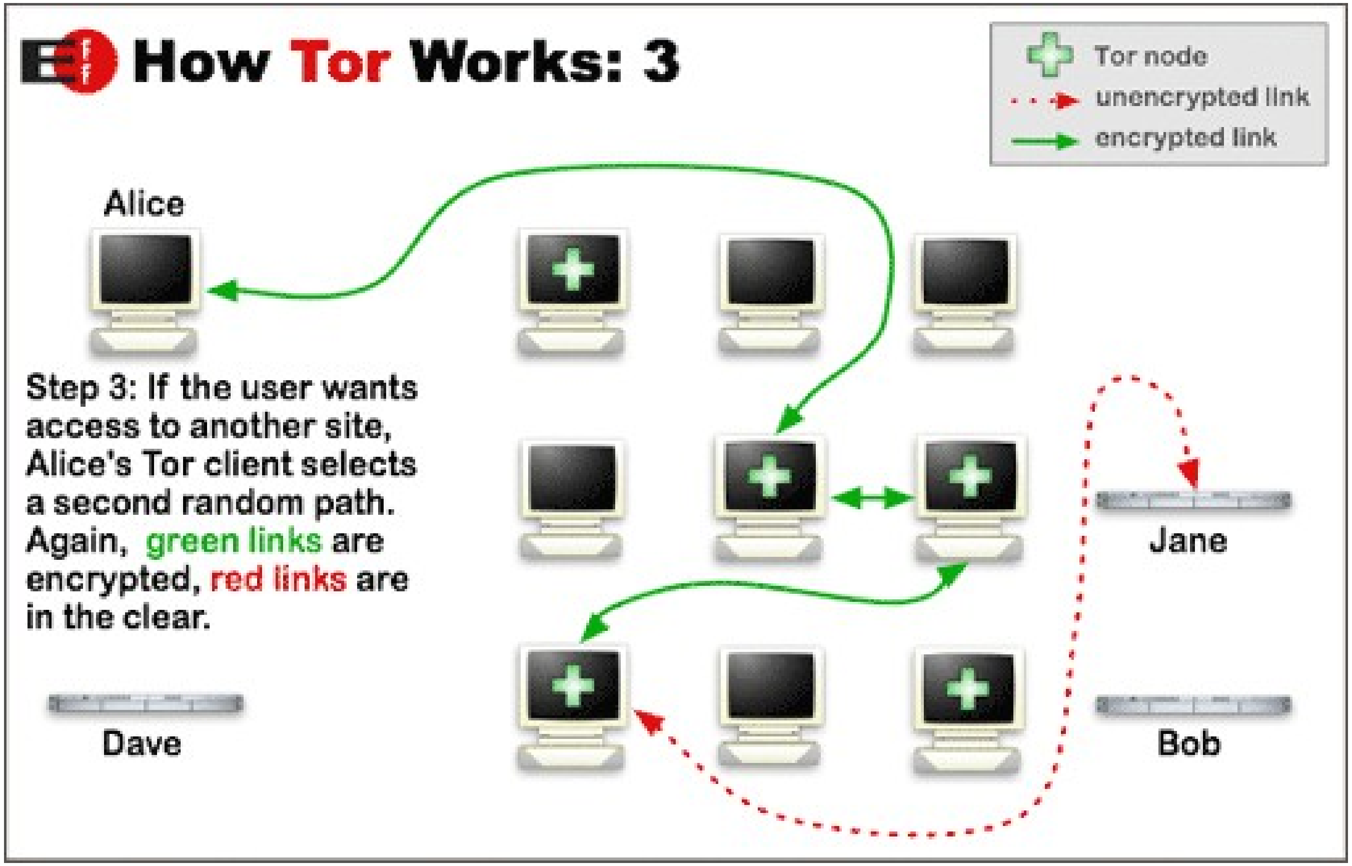
http://tor.eff.org

How Tor Works II


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

http://tor.eff.org

How Tor Works III



How Tor Works: 3

Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

http://tor.eff.org

Attacks on Tor

Evil Exit Node

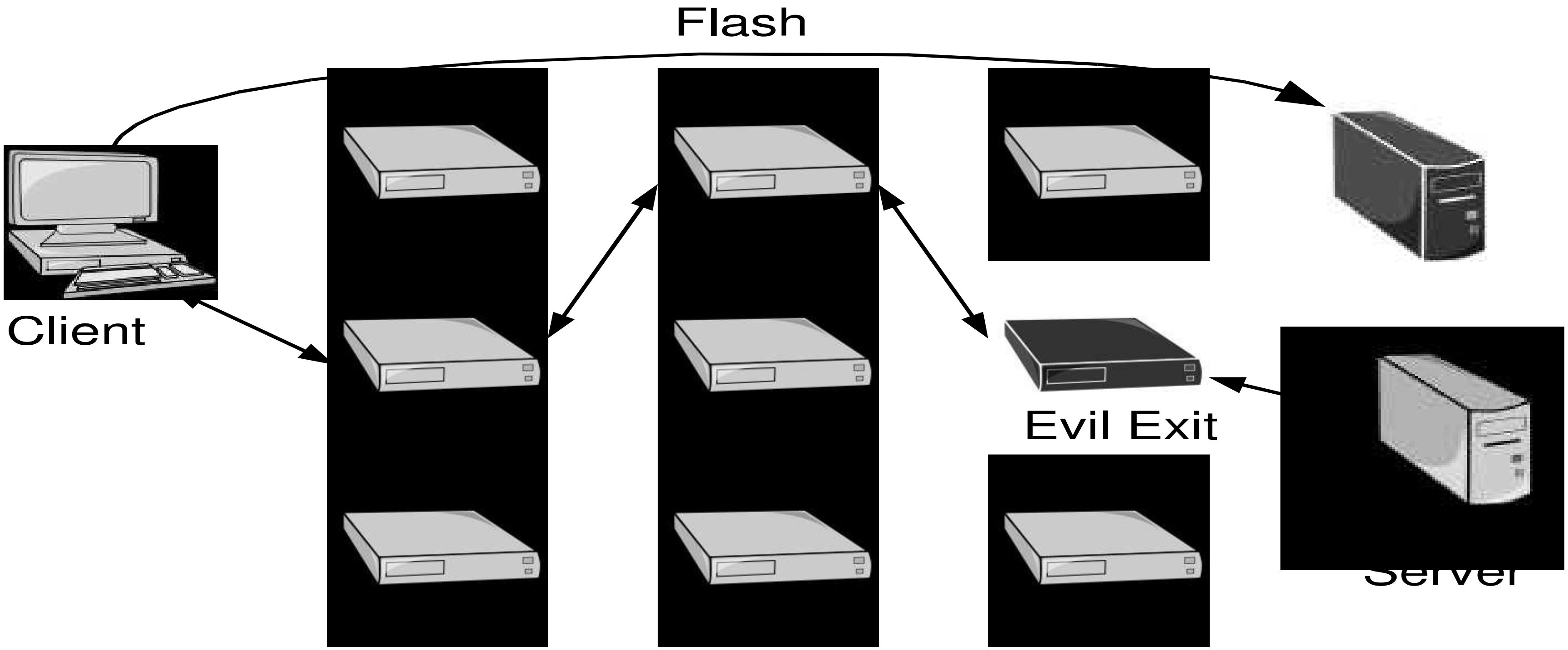


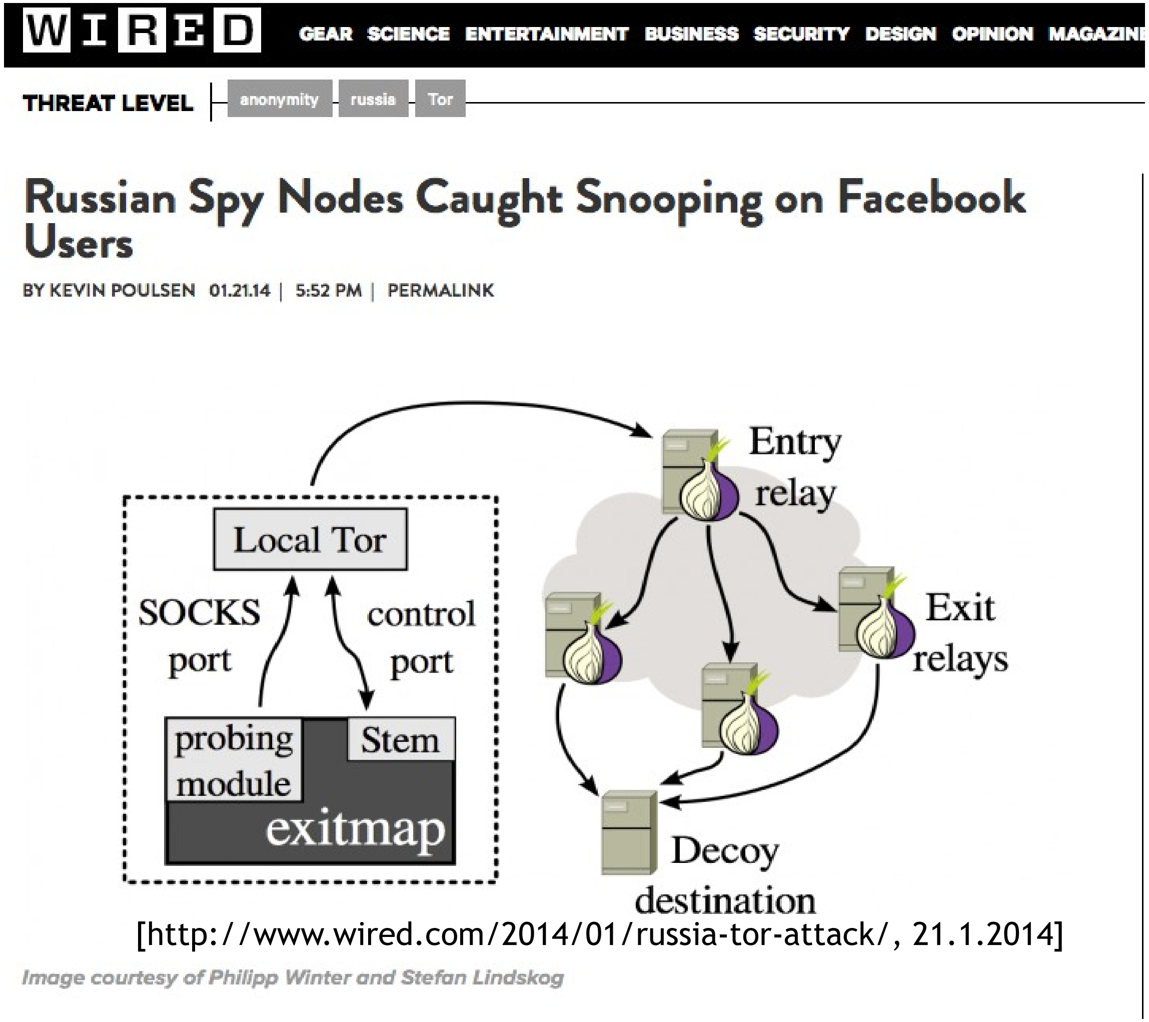
Fig. 3. A browser attack executed by an exit node. The client's web browser executes a Flash program inserted into a webpage by the exit node, which opens a direct connection to a logger machine.

[AbLa2007]

Attacks on Tor

Evil Exit Node Attack Materialized

- Almost 20 exit relays in the Tor anonymity network that attempted to spy on users' encrypted traffic using man-in-the-middle techniques.
- Exit relays detected sniffing the traffic (both HTTP and SSL sniffing attacks)



WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZIN

THREAT LEVEL | anonymity russia Tor

Russian Spy Nodes Caught Snooping on Facebook Users

BY KEVIN POULSEN 01.21.14 | 5:52 PM | PERMALINK

Image courtesy of Philipp Winter and Stefan Lindskog

[http://www.wired.com/2014/01/russia-tor-attack/, 21.1.2014]

Attacks on Tor

Evil Web Server

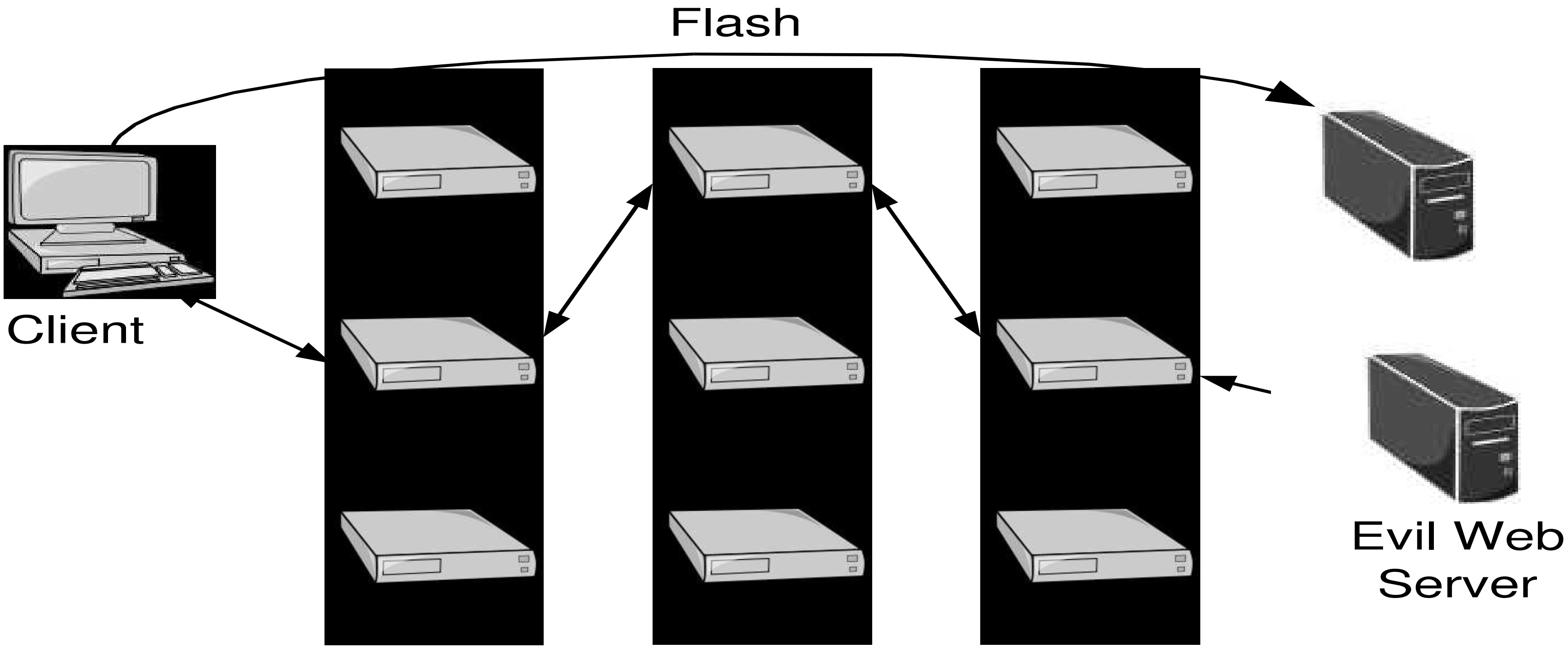
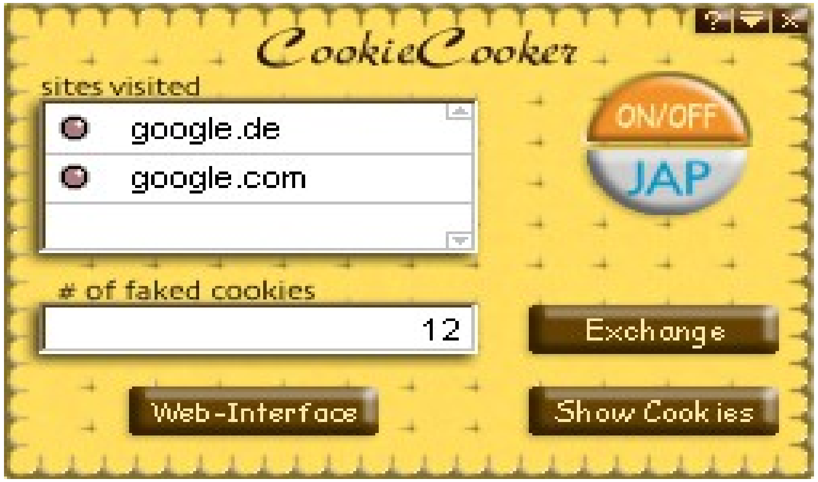


Fig. 2. A browser attack using Flash included in a website. The client's web browser executes a Flash program, which then opens a direct connection to a logger machine, compromising the client's anonymity.

[AbLa2007]

CookieCooker

- Confuse data collectors
  - Exchange of cookies between users
  - Exchange of identities
  - Use of „faked“ data
- User-defined identity management
  - Assistance for the registration
  - Application of „real“ and „faked“ data
- Spam protection through disposable email addresses
- Ad blocking
- Integrated with JAP Anonymizer



sites visited

- google.de
- google.com

# of faked cookies: 12

Cryptography II and Network Security II

Some slides were skipped during his lecture in Cryptography II & Network Security II. Do we still need to learn them?

- The lecturer emphasized on main points and concepts that need elaboration.
- The lecturer might have briefly explained other details that students could go through the slides themselves using their notes or some course book.
- If you have concrete questions, please send them to sec@m-chair.de.

Access control

Lecture on Access Control: Slide 21: Is the content of this slide the criticism of the Capability List? Is there any similar criticism for the Access Control List?

Capabilities

- Complexity of security management by capabilities is very high.
- Operating systems are traditionally oriented towards managing objects.
- It is difficult to get an overview of who has permission to access a given object.
- It is very difficult to revoke a capability.

[Go99]

Back to the question

- Q: Lecture on Access Control: Slide 21:
  - *Q1: Is the content of this slide the criticism of the Capability List?*
  - *Q2: Is there any similar criticism for the Access Control List?*
- A:
  - A1: Yes, the slide lists the weaknesses of capability lists.
  - A2: Yes, e.g. Access Control Lists may be more difficult to edit (add, delete) a subject from the access control list of an object. But the nice thing is that revocation to an object can easier be managed.

Cryptography II

RSA

- Q: *Should we be able to calculate the modulo formula for asymmetric encryption (RSA)*?
- A: You should know what modulo operation is and how to calculate it. This is regardless of RSA.

RSA (2)

- Q: *How detailed do we have to know the RSA encryption? We just had one example in the slides and no exercises.*
- A: Knowing the logic behind the simplified example from the lecture is enough. You do not need to perform the calculations, e.g. modular exponentiations.

Q: How exactly do I determine *e*? Can this be computed?

Choosing the Keys (I)

- You first compute ***n*** as the product of two primes ***p*** and ***q***.
- ***n=p*q***
- These primes are very large “random” primes.
- Although you will make ***n*** public, the factors ***p*** and ***q*** will be effectively hidden from everyone else due to the enormous difficulty of factoring ***n***.
- This also hides the way, how ***d*** can be derived from ***e***.

[RSA78]

Choosing the Keys (II)

- You then choose an integer ***d*** to be a large, random integer which is relatively prime to ***(p-1)*(q-1)***.

- That is, check that ***d*** satisfies:
  - The greatest common divisor of `d` and `(p-1)*(q-1)` is `1`, namely that `gcd(d,(p-1)*(q-1))=1`

[RSA78]

Choosing the Keys (III)

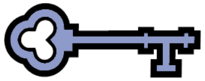
- The integer ***e*** is finally computed from ***p***,***q***, and ***d*** to be the "multiplicative inverse" of ***d***, modulo (***p-1***)*(***q-1***).

- Thus we have

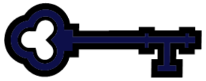
  $$e*d \frown 1 \ (\mathrm{mod}\ (p-1)*(q-1)).$$

[RSA78]

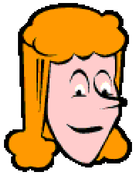
Simplified Example (I)



Public
(e,n)



Private
(d,n)



Alice

- Let p=7 and q=11.
- Then n=77.
- Alice chooses d=53, so e=17.
  - HINT: *e* can be calculated using the Extended Eucledian Algorithm, which is out of the scope of the course.
- `gcd(d,(p-1)*(q-1)) = gcd(53,(7-1)*(11-1)) = gcd(53,60) = 1`
- `e*d mod (p-1)*(q-1) = 901 mod 60 = 1`

Based on [Bi05]

Certification of Public Keys – Web of trust

- Q: *Web of Trust: Whose public key is used when?*
- A: Take the example of PGP, where the concept originally comes from. Each user can “vouch” for the public key of other users in the sense of the trust they have that a certain public key is indeed mapping to the name/identity of a given person/institution. Hence the “trust” in the name of the concept.

Electronic signatures

Electronic signatures

- Q: *Lecture on Electronic Signatures: Slide 25- 27: In how far do we need to know legal constructs and laws?*

- A: Focus on understanding the concepts behind them rather than remembering them all by heart, especially the European regulation on certificates and signatures.

General Questions

General questions

- Q: *In how far do we need to draw things and explain things with drawings?*
- A: Question too general. In principle, you should recognize the important components in different graphs or diagrams that are useful to illustrate the concept. Usually we specify whether we expect a drawing only or also explanation.

- Q: *There so many slides we discussed in the lecture. Where should we focus? How detailed do we have to know everything? (Legal frameworks, technical specs, etc)*
- A: Question too general. Mostly you should demonstrate the understanding of the concepts, but some questions may require naming or explaining specific technical or legal concepts.

Deutsche Telekom Chair of Mobile Business & Multilateral Security

J. Serna-Olvera, W.B. Tesfay and F. Veseli
sec@m-chair.de
Goethe University Frankfurt
E-Mail: {jetzabel.serna-olvera, welderufael.tesfay, fatbardh.veseli}@m-chair.de
WWW: www.m-chair.de