Information & Communication Security (WS 16/17)

Questions and answers – Exam preparation

Kai Rannenberg, Ahmed S Yesuf and Majid Hatamian
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

mobile business

Question 1

Please explain the difference between ABC4Trust, Idemix and U-Prove.

ABC4Trust

- Attribute-Based Credentials for Trust: https://www.abc4trust.eu
- Coordinated by Goethe University Frankfurt
- 12 partners from 7 countries
- Objectives:
  - to define a common, unified architecture for ABC systems to allow comparing their respective features and combining them on common platforms, and
  - to deliver open reference implementations of selected ABC systems and deploy them in actual production pilots allowing provably accredited members of restricted communities to provide anonymous feedback on their community or its members.

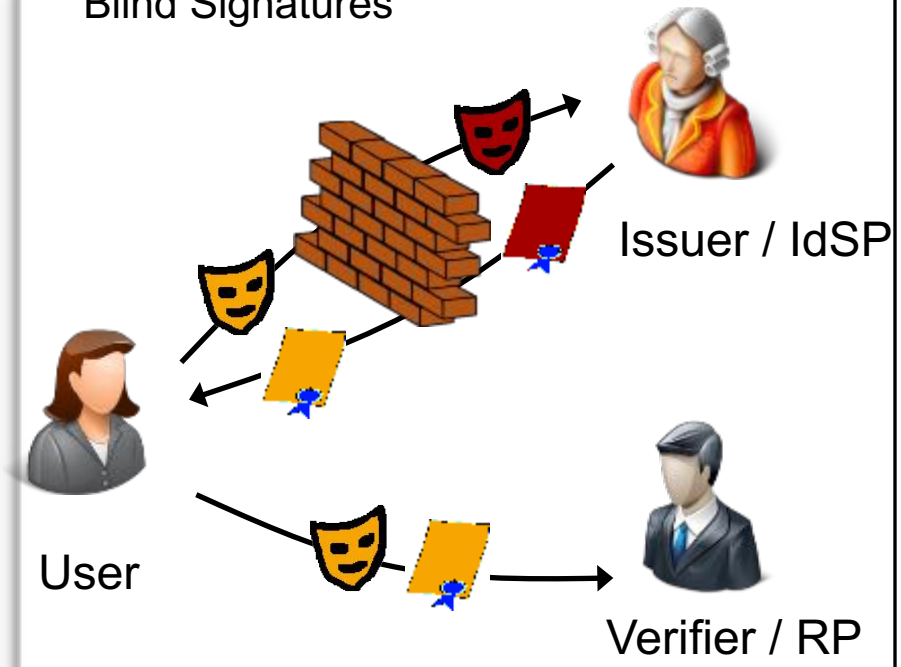
Credential Systems

Privacy-enhancing Attribute-based Credentials (Privacy-ABCs)

- Privacy features:
  - Different levels of pseudonymity
  - Selective (minimal) disclosure of attributes (attribute hiding)
  - Unlinkability of user's transactions
- Additional features are possible:
  - Prove age without disclosing birthday, e.g. for buying alcohol, showing being over 18
  - Proving of not being revoked, without disclosing the serial number in the credential
  - Predicates over attributes (no disclosure) with a constant value or another attribute
    - Inequality of attributes
    - Equality of attributes
    - Value belonging to a certain interval
  - Controlled linkability, e.g. avoid voting more than once
  - Conditional accountability, when needed

Two approaches for Privacy-ABCs

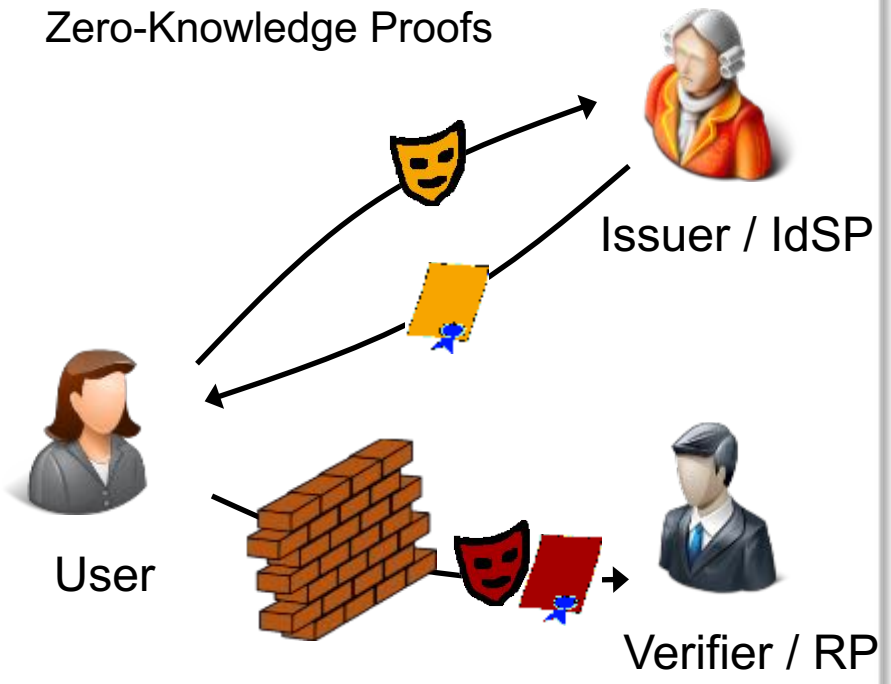
Blind Signatures



U-Prove

Brands, Paquin et al.
Discrete Logs, RSA,..

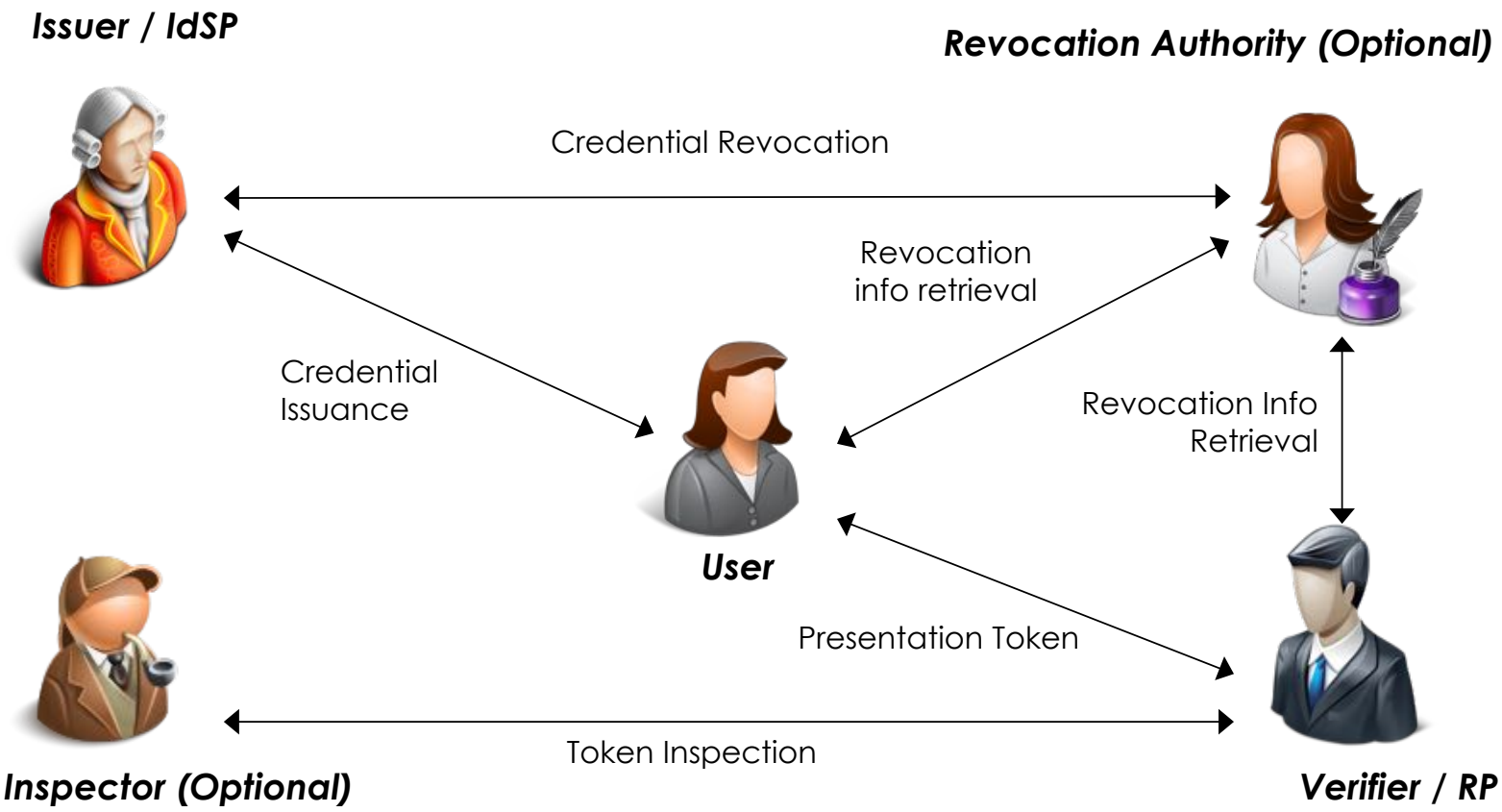
Zero-Knowledge Proofs



Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)

ABC4Trust architecture
High level view



mobile business

Question 2

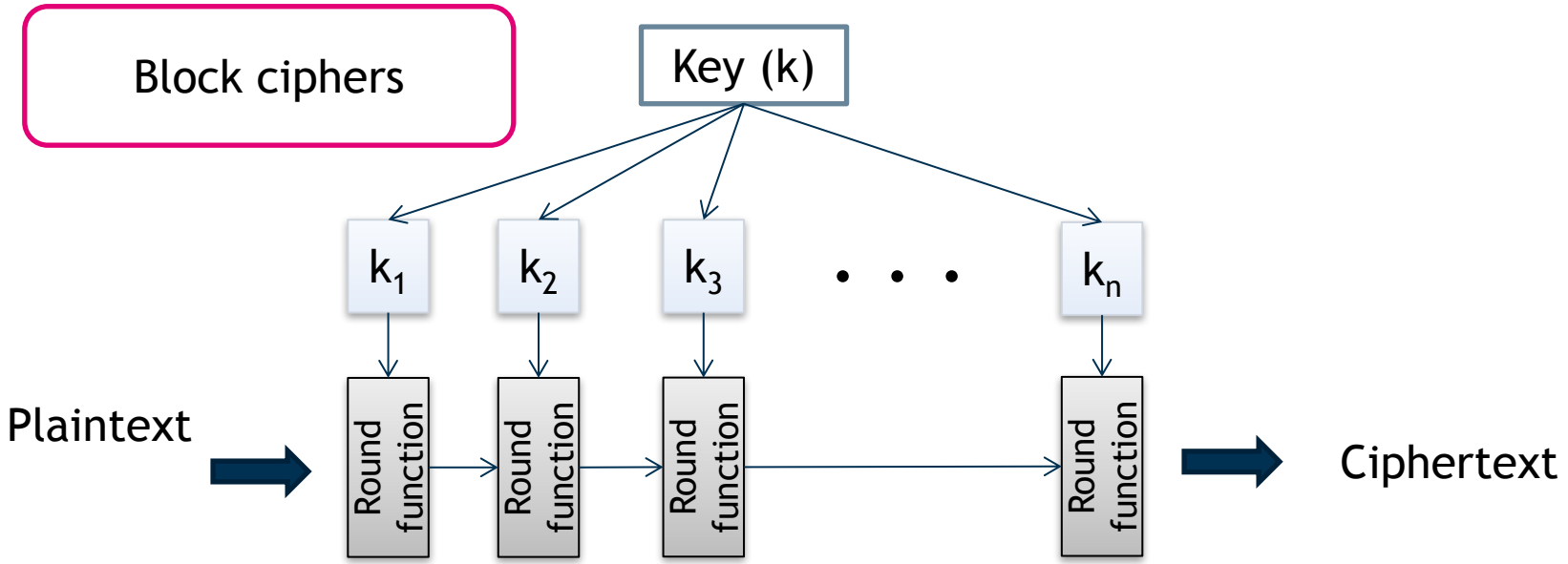
How detailed do we have to know the underlying principle of AES and RSA?

Advanced Encryption Standard (AES) – History

- The Data Encryption Standard (DES) was designed to encipher sensitive but not classified data.
- The standard has been issued in 1977.
- In 1998, a design for a computer system and software that could break any DES-enciphered message within a few days was published.
- By 1999, it was clear that the DES no longer provided the same level of security it had 10 years earlier, and the search was on for a new, stronger cipher.
- AES Rijndael was a winner of U.S. National Institute of Standards and Technology bid for advanced encryptions.
- AES has been approved for Secret or even Top Secret information by the NSA.

[Bi05]

AES – Functionality



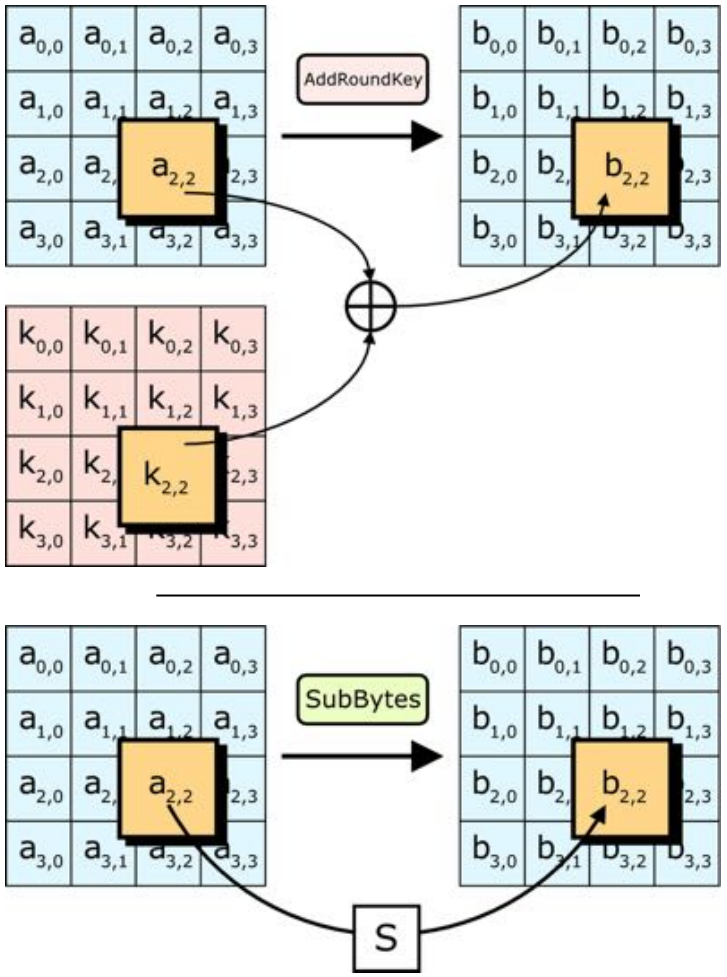
- Variable **number of rounds (10, 12, 14)**
- Depending on **key size (128-bit, 192-bit, 256-bit)**.

[Bi2005]

Encryption Round (1)

AES

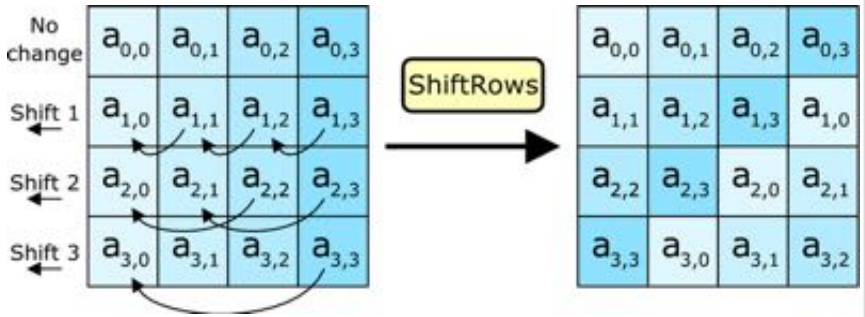
- AddRoundKey
  - XOR (mix bits of) current state a and round key
  - Round key k derived using key schedule
- SubBytes
  - Substitution using a lookup table (S-Box)

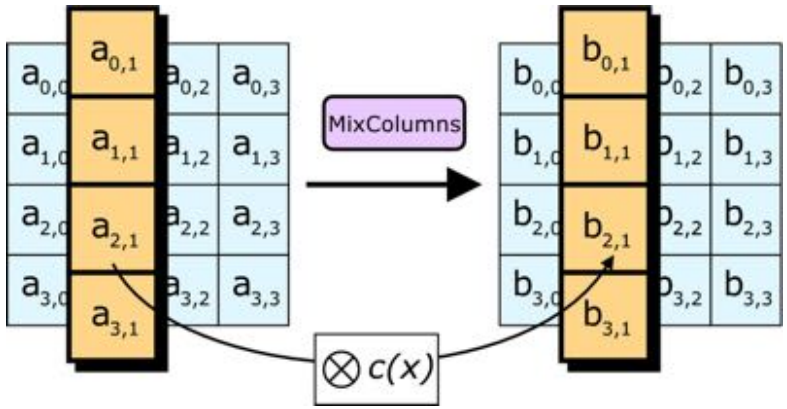


Encryption Round (2)

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)]
  - GF = Galois field = finite field





mobile business

RSA

RSA Encryption

- To encrypt a message M, using a public key (e,n), proceed as follows (e and n are a pair of positive integers):
  - First represent the message as an integer between 0 and $n-1$ (break long messages into a series of blocks, and represent each block as such an integer).
  - Then encrypt the message by raising it to the e^{th} power modulo n.
  - The result (the ciphertext C) is the remainder of M^e divided by n.
  - The encryption key is thus the pair of positive integers (e,n).

[RSA78]

mobile business

RSA Decryption

- To decrypt the ciphertext, raise it to another power ***d***, again modulo ***n***.
- The decryption key is the pair of positive integers (***d***,***n***).
- Each user makes his encryption key public, and keeps the corresponding decryption key private.

[RSA78]

RSA Encryption/Decryption Summary

- $C \equiv E(M) \equiv M^e \pmod{n}$, for a message M
- $M \equiv D(C) \equiv C^d \pmod{n}$, for a ciphertext C

[RSA78]

Choosing the Keys (I)

- You first compute ***n*** as the product of two chosen 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]

mobile business

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`.
  - `gcd(d,(p-1)*(q-1))=1`

[RSA78]

mobile business

Choosing the Keys (III)

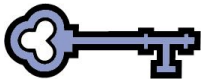
- The integer ***e*** is finally computed from ***p***,***q***, and ***d*** to be the "multiplicative inverse" of ***d***, modulo (***p-1***)***(***q-1***).

- Thus we have

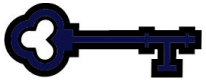
$$e*d \equiv 1 \pmod{(p-1)*(q-1)}.$$

[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.
- `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]

Simplified Example (II)

- Bob wants to send the message „HELLO WORLD“ to Alice.
- Each plaintext character is represented by a number between 00(A) and 25 (Z).
- Therefore, we have the plaintext as:

```
07 04 11 11 14 26 22 14
17 11 03
```

HELLO WORLD

Bob

Based on [Bi05]

Simplified Example (III)

- Using Alice's public key the ciphertext is:
  - $07^{17} \bmod 77 = 28$
  - $04^{17} \bmod 77 = 16$
  - $11^{17} \bmod 77 = 44$

  …
  - $03^{17} \bmod 77 = 75$
- Or 28 16 44 44 42 38 22 42 19 44 75

HELLO WORLD

Bob

Based on [Bi05]

Simplified Example (IV)

28 16 44 44
42 38 22
42 19 44 75

- Alice decrypts the ciphertext by calculating:
  - $28^{53} \bmod 77 = 07$
  - $16^{53} \bmod 77 = 04$
  - $44^{53} \bmod 77 = 11$

  …
  - $75^{53} \bmod 77 = 03$
- Or: 07 04 11 11 14 26 22 14 17 11 03 = “HELLO WORLD”

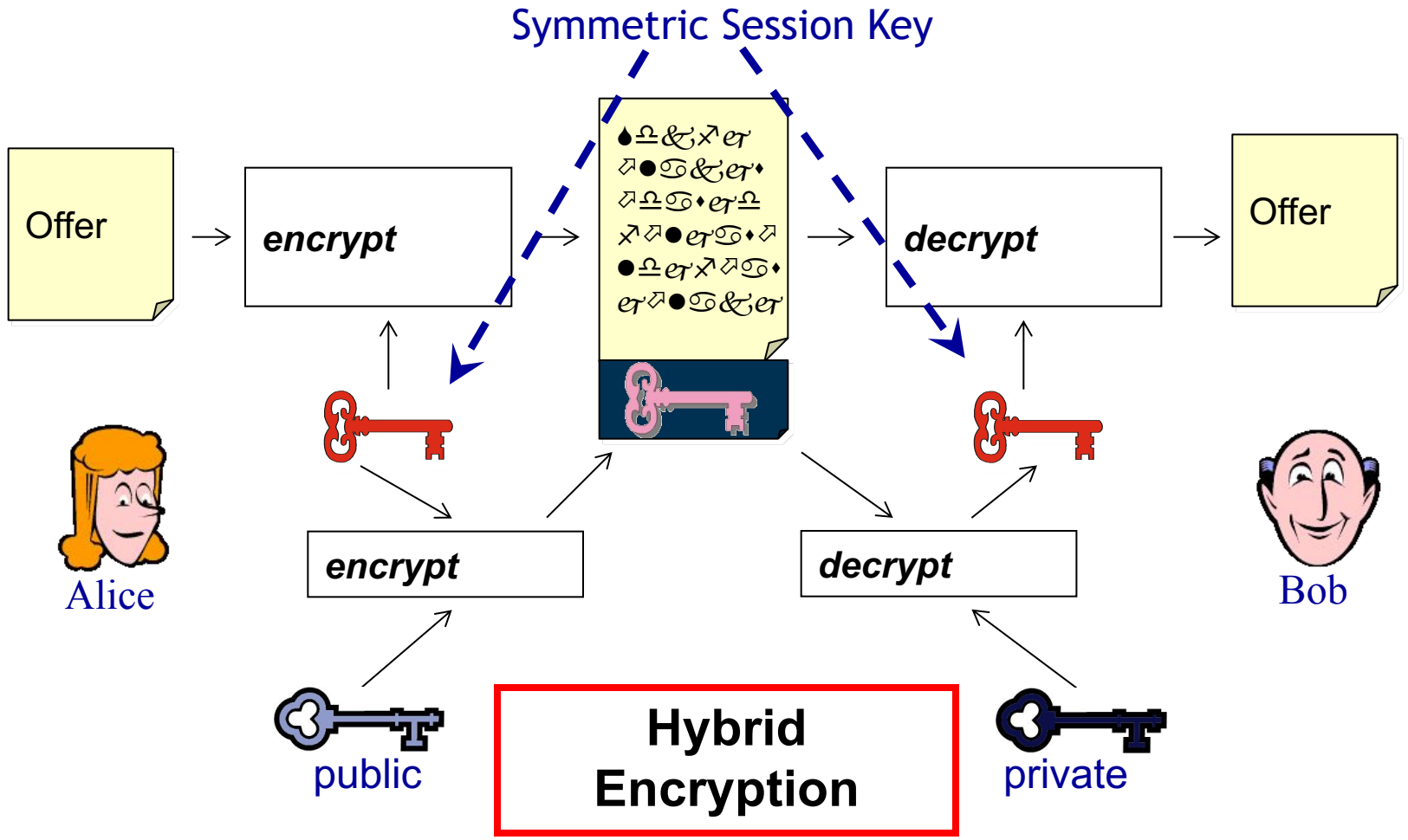
Based on [Bi05]

mobile business

Question 3

Please explain a hybrid encryption system (lecture 05 slide 25).

Solution: Hybrid Systems



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

mobile business

Question 4

Please explain the “presentation problem” (lecture 06, slide 41).

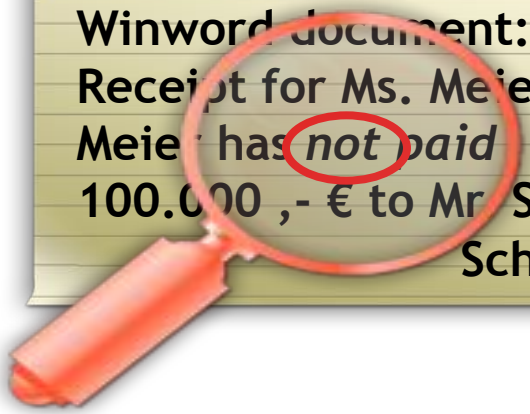
Presentation Problems

Mr. Schulz

Winword document
Receipt for Ms. Meier:
Ms. Meier has paid
100.000 ,- € to Mr. Schulz.
Schulz

Ms. Meier

Winword document:
Receipt for Ms. Meier: Ms.
Meier has *not paid*
100.000 ,- € to Mr. Schulz.
Schulz



But check for hidden text !!!!

[Based on IsRo]

mobile business

Question 5

Assignment 3, Exercise 3b: Why is b1 not suitable to encrypt the plain text? b1 is one digit longer than the plain text, but couldn't that digit simply be cut off?

Exercise 3: Stream ciphers

- b) Alice wants to encrypt the letter A, where the letter is given in ASCII code. The ASCII value for A is $65_{10} = 1000001_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext:
  - b1) 10100110
  - b2) 0011111
  - b3) 101010

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

Truth Table of the XOR operation

[MPS11]

Exercise 3: Stream ciphers

- c) Encrypt the message using Vernam code and using XOR as an encryption function and the key in b).

Plaintext (A)	1000001
Key (B)	0011111
Ciphertext (A xor B)	1011110

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

Truth Table of the XOR operation

mobile business

Literature

- **[Bi05] Bishop, Matt:** *Introduction to Computer Security.* Boston: Addison Wesley, 2005. pp. 113-116.
- **[RSA78] Rivest, Ron L., Shamir, A. and Adleman, L.:** A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, February 1978, 21(2), pp. 120-126.
- [MPS11] Alfred J. **Menezes, Paul C. van Oorschot and Scott A. Vanstone:** Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/, pp. 274.

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Kai Rannenberg, Ahmed S Yesuf and Majid Hatamian

sec@m-chair.de

Goethe University Frankfurt

E-Mail: {kai.rannenberg, ahmed.yesuf, majid.hatamian}@m-chair.de

WWW: www.m-chair.de