Cryptography

Prof. Dr. Werner Schindler

Federal civil servant at
Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Bonn

Adjunct Professor
(außerplanmäßiger Professor)
at Darmstadt University of
Technology

B-IT, winter 2006 / 2007

Structure of the Course

Chapter A: Introduction

Chapter B: Symmetric Ciphers

Chapter C: Public Key Cryptography

A) Introduction

A.1 Development of Cryptography

- The history of cryptography dates back more than 2000 years ago.
- Already Julius Cesar encrypted important messages (Sueton, Roman historian).

A.2 Julius Cesar‘s Cipher (I)

JDOOLD HVW RPQLV GLYLVD ...

plaintext alphabet: ABCDEF**G**HIJKLMNOPQRSTUVWXYZ

ciphertext alphabet: DEFGHI**J**KLMNOPQRSTUVWXYZABC

GALLIA EST OMNIS DIVISA ...
[Translation: Gallia (today’s France) is divided into three parts ...]

A.2 Julius Cesar‘s Cipher (II)

- Cesar‘s cipher defines an encryption scheme in a modern sense (though a very weak one).
- It applies an algorithm to transfer plaintext into ciphertext, using a key
- Algorithm:
  - rotate the plaintext alphabet by k (= key) positions to the left (= ciphertext alphabet)
  - substitute the plaintext letter by the corresponding ciphertext letter
- Cesar used the key k = 3

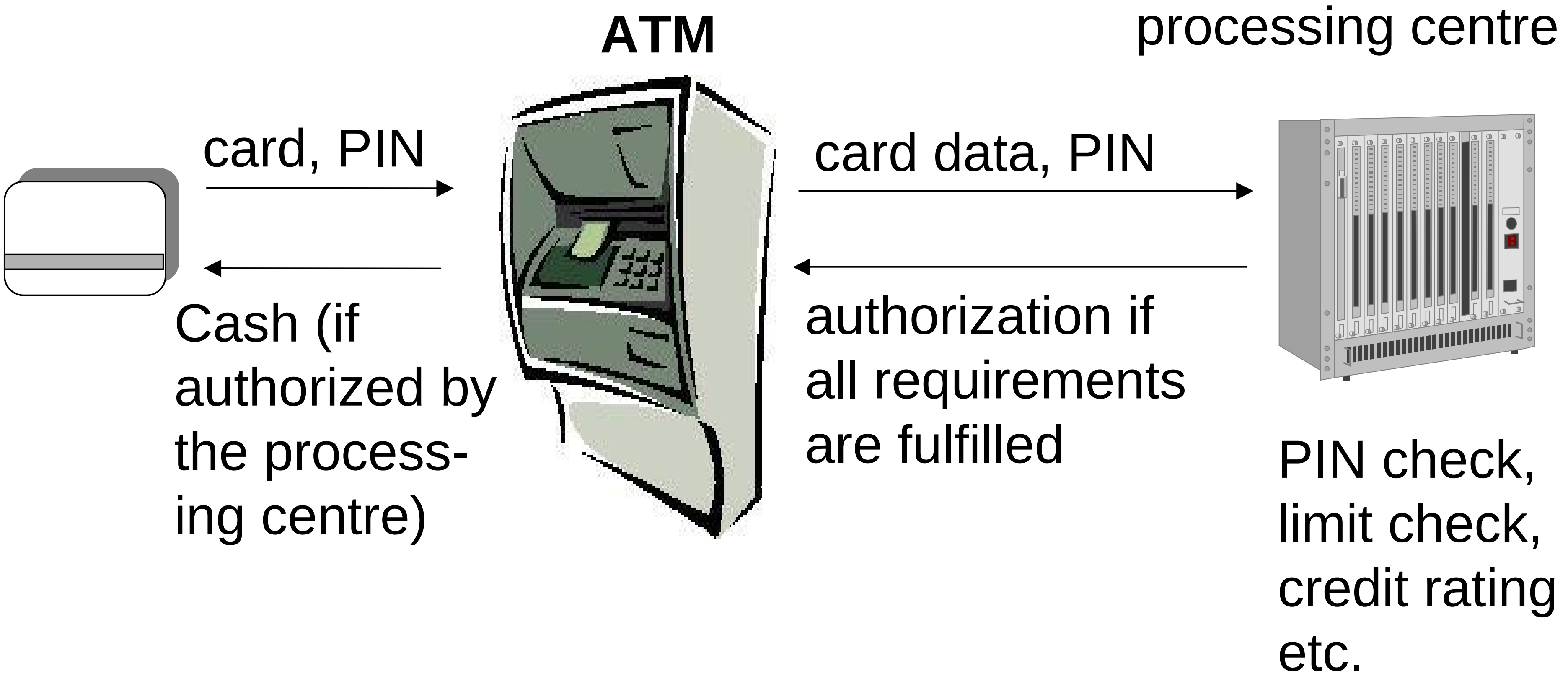
A.1 (continued) Development of Cryptography (II)

- It is very easy to break Cesar‘s cipher: An attacker just has to decrypt a given ciphertext with all 26 admissible keys. Only one key (the correct key) yields meaningful plaintext.
- Cryptographic algorithms have been attacked, broken and improved for the last 2000 years.
- Before the eighties cryptography was mainly applied by the military and intelligence services.

A.3 Cryptography in everyday‘s life

- By the spreading of smart cards and the internet cryptography has found its way into our daily life although we are often not aware of this fact.
- Examples:
  - w Bank cards and credit cards at automated teller machines
  - w Home banking, e-commerce
  - w Credit card transactions over the internet
  - w Mobile communication
  - w Electronic purses (smart cards)
  - w …

A.4 Example a) Automated teller machines (ATMs)



ATM

processing centre

card, PIN

Cash (if authorized by the processing centre)

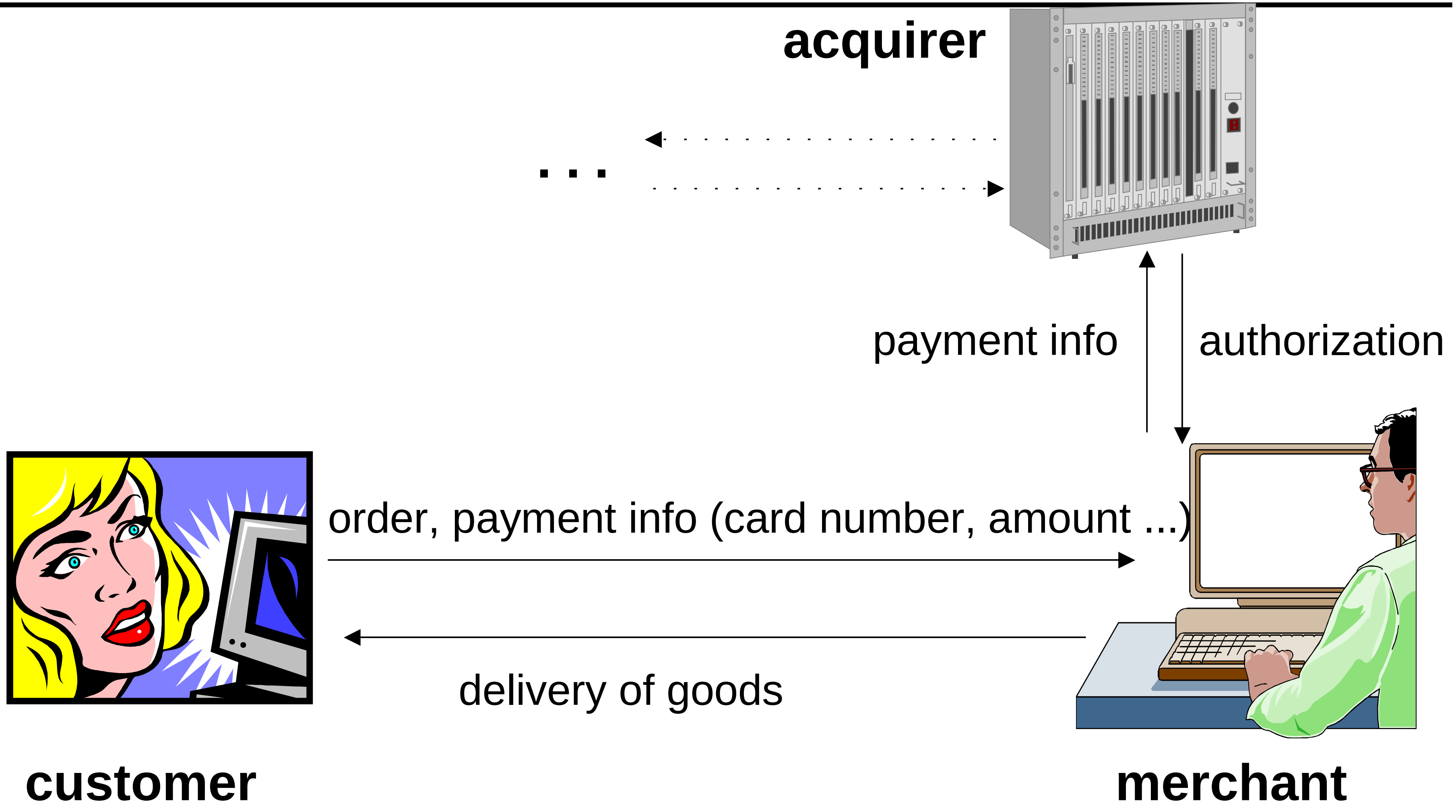
card data, PIN

authorization if all requirements are fulfilled

PIN check, limit check, credit rating etc.

Remark: The ATM encrypts the entered PIN before transmission.

A.4 b) Credit card payment over the internet



acquirer

...

payment info

authorization

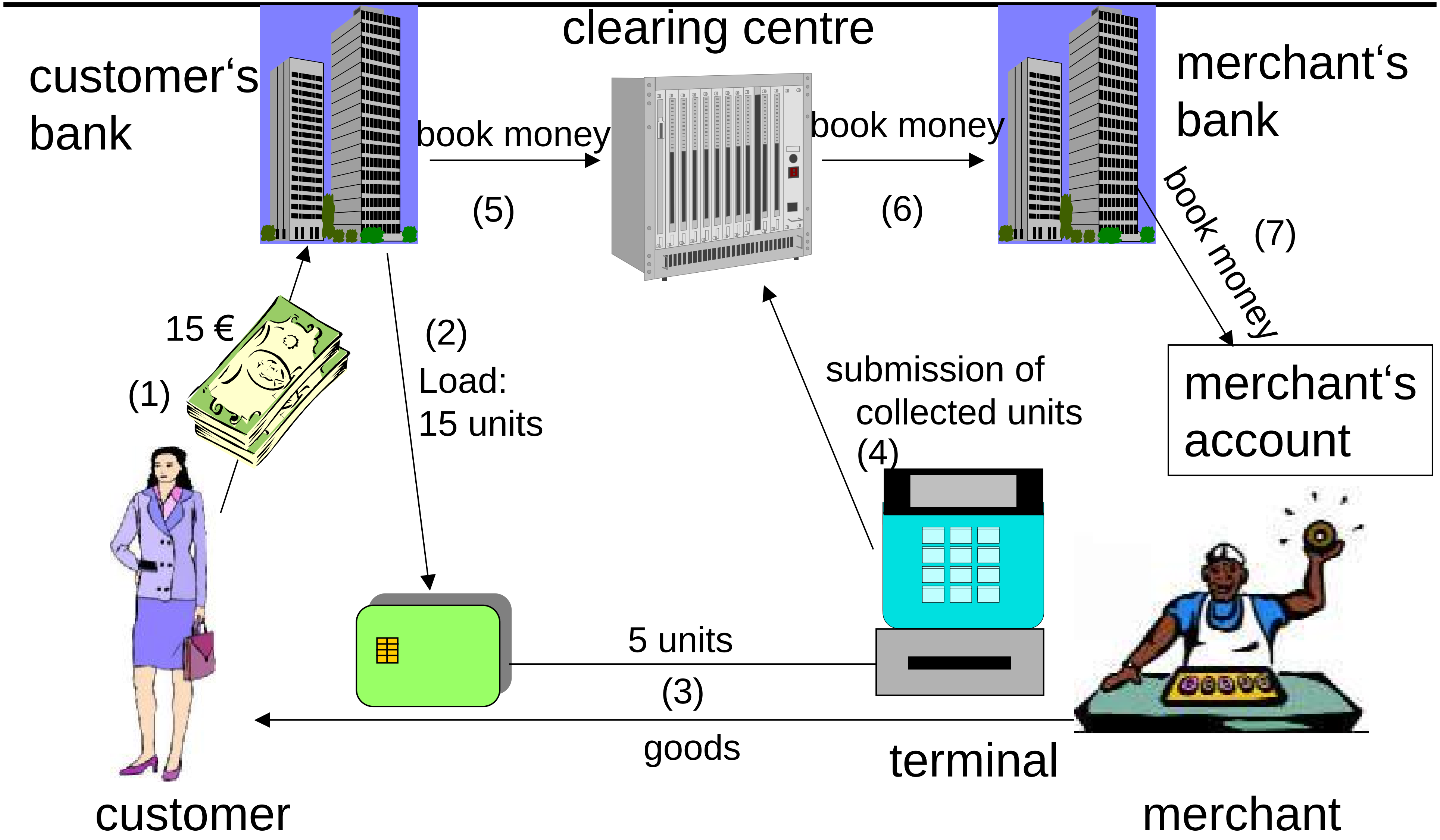
order, payment info (card number, amount ...)

delivery of goods

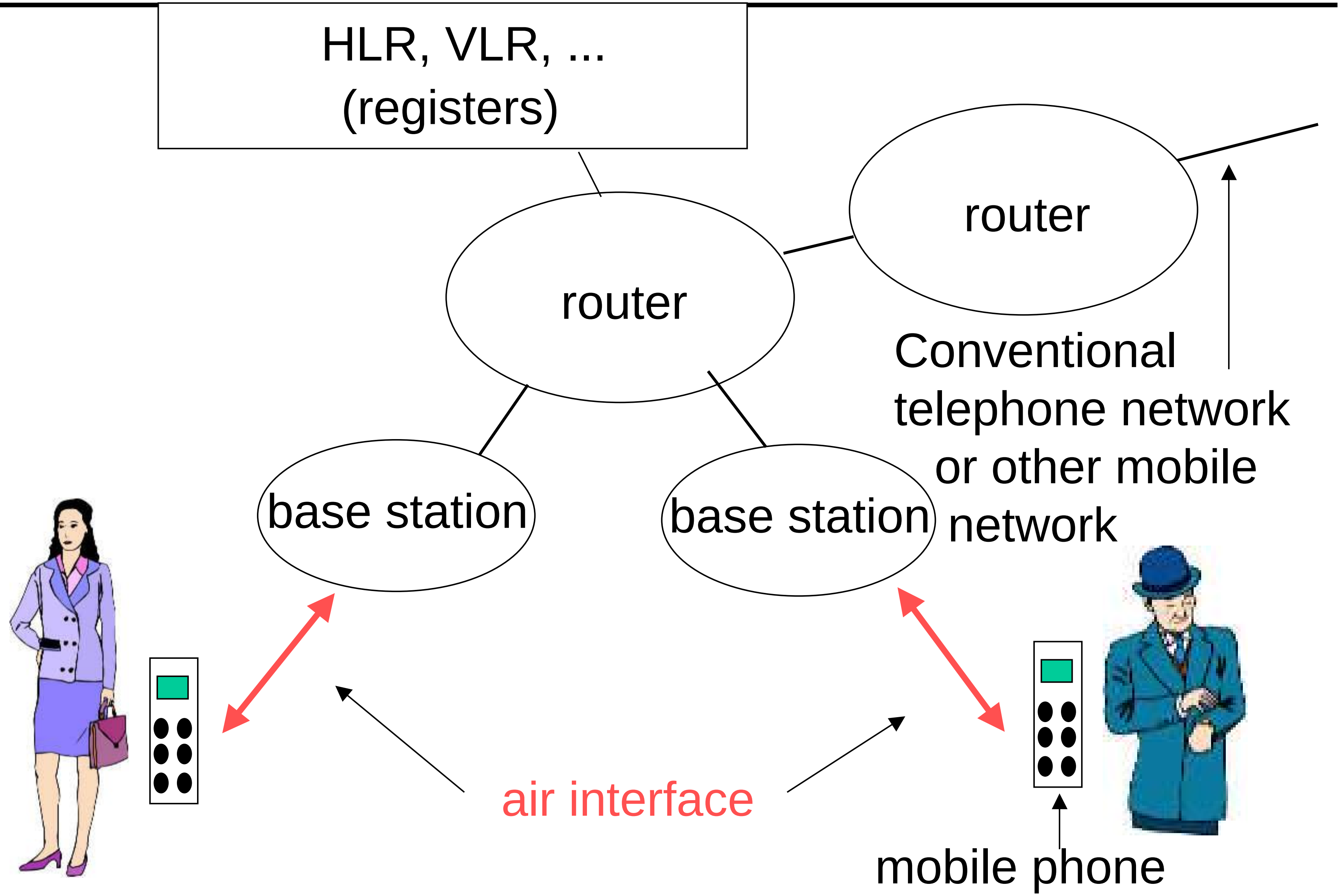
customer

merchant

A.4 c) Electronic purse system



A.4 d) GSM mobile phone



A.5 Important Security Requirements

Requirement / desired property	Bank cards / credit cards at ATMs	Credit card payment over the internet	Electronic purse systems	Home banking	Mobile communication
to be kept secret	PIN	credit card number		PIN / TAN	PIN, transmitted data
data integrity	account number, amount	price, delivery address	records	amount, destination	yes
authentication	card holder – processing centre, ATM – processing centre, …	merchant – card holder, merchant – acquirer, …	purse – terminal, terminal - purse, …	account holder - bank	user – SIM card, SIM card - network
non-repudiation	yes	yes	no	yes	yes
long-term storage of data	transaction protocols	transaction protocols	system-dependent	trans-action records	no

A.6 Remark

- Security requirements as secrecy, data integrity and authenticity, for instance, can be assured by cryptographic algorithms and protocols.
- This will be the focus of this course. As far as possible these mechanisms will be motivated and illustrated by applications.
- We point out that even strong cryptographic mechanisms may be overwhelmed if there are flaws in their implementation (Keywords: hardware attacks, side-channel attacks, fault attacks, cache-based attacks, bugs in the network protocol, vulnerability to viruses, worms and trojan horses, weaknesses of the operating system, …).
- In this course we will not consider these topics.

A.7 Some Further Historical Notes

- Maria Stuart (1542-1587, Queen of Scotland) was sentenced to death because of weakly enciphered letters.
- In the Renaissance cryptography belonged to the esoteric arts.
- Cryptography in literature: In “The Gold Bug” (E.A. Poe), for instance, a solved cryptogram reveals the location of a treasure.
- During the second world war the allies broke the German Enigma, a mechanical enciphering machine. This was maybe the greatest cryptanalytic success in the 20th century.