grades: 40% lecture, 60% lab

exam, no tests during the course, exam in English unless...

short problems, skills examined not knowledge

lower bound: 40% 3, 50% 3.5, 60% 4, 70 % 4.5 80% 5.0

## SMART CARDS

**types of no-smart solutions:**

- **embossed**
- **magnetic:** 1000 bits, 3 tracks, track 1: 79 6bit chars, track 2: 40 4bit chars, track 3: 107 4-bit chars, limited density (movement in reader against the head), standard data, track 3 for read-write, no physical protection, cheap readers, horror as ATM cards

**smart cards:**

- memory cards (with security logic and without)
- processor: with coprocessor (NPU) or without (RSA in 20 minutes)
- contact or wireless
- multimegabyte

**optical:**

- writing technique - like CD
- designated field according to standards
- megabytes
- redundancy, therefore not easy to destroy information (border control cards)

**contacts**:

- 8 fields, normally 6 used (2 for future applications), places for contacts strictly determined in standard
- ground, voltage, I/O, clock, CTRL
- easy to destoroy
- corrosion, mechanical scratches, not for intensive use

**Wireless:**

- well sealed for corrosion
- reader may activate from distance

- response with low energy, recognizable from a short distance only

**Material**:

PVC: polivinyl chloride, credit cards, cheap, lifetime 2 years, cost 1

ABS: mobile, termally stable, up to 100 C, laser engraving poor, 3 years, cost 2

PC: polycarbonate, ID cards, durable, 160 C, problems with hot stamping, lifetime 5 years, cost 7, low scratch resistance,

PET: healtch cards, mechanical: very good resistance, lifetime 3 years, cost 2.5

**Graphical security means:**

- Guilloche
- colored signature field
- microtext
- ultraviolet
- barcode
- hologram
- kinegram
- embossing
- laser engraving (surface or inside)

---

**Memory**:

EPROM - UV erasure, problematic in smart cards,

EEPROM - electrical erasure, cell capacitors, erase state -> non-erased (single bit), non-erased-> erased: page or sector, both slow, size 1.14 mi m, 100.000-1.000.000 erasures, 2-10ms

flash - hot electron injection, write time „flash", erase like EEPROM, size 0.47,

10.000-100.000 erasures, 10 microsec

RAM - transistors, flip-flop, size 1.87 mi m, erasures - unlimited, write: 70ns

ROM - connections

**UNITs:**

UART - universal asynchronous receiver transmitter, software solutions too slow

USB

SWP single wire protocol

timer

CRC cyclic redundancy clock, Reed Solomon codes, $p_x(a) = \sum x_i a^{i-1}$, $c(x) = p_x(a_1)p_x(a_2)....$

$C(x) = x \cdot A$, Vandermode matrix, row 1: 1....1, row2: $a_1, .... a_n$, row 3: $a_1^2$, ...,$a_n^2$, and so on

RNG temperature etc. hard to implement, pragmatic solutions: PRNG (sometimes poor), be aware that the algorithm implemented is not original one (e.g. DSA but DSA+LFSR+...), PRNG: with the key from previous values.

- Round Robin- eg 12 values in a buffer
- EEPROM counter increased after each reset, Enc(counter)
- testing - NIST tests, value problematic

MMU memory management unit

JAVA accelerator: native instruction set, 1) dedicated hardware component, hish speed but takes place, 2) native instructions for java

Symmetric crypto coprocessor: 75 microseconds per DES, 150 per 3DES

asymmetric coprocessor: RSA up to 2048,

- ChRC
- only with NPU
- problematic key generation, probabilistic time

EC 160-256 bits

- DSS
- random numbers

hash functions:

- NIST, Keccak in smartcards
- no update, SHA1 in Poland

memory for keys:

- masterkey, derived keys, dynamic keys (session)
- PIN: master or deriving from master key, PIN updates in different memory, problems of nonuniformity of PIN (no leading zeroes, etc), subclasses where strategy gives higher chances

---

Fabrication:

big series, large scale, few machines

multichip: vertical system integration

chip-on-flex modules: stepwise on a large number of chips at the same time, complicated wiring, ...

lead-frame: integrated

Electrical:

supply problems: 3V batteries for mobile phones , types 1.8, 3V 5V

maximum current: example 50mA, hardware protection against too high voltage

contacts: supply, reset, clock, aux for USB, ground, SPU (proprietary or standards, SWP in telecommunication), I/O, aux2 for USB

clock: tolerance rate 40-60%, clock divider