Daffodil International University

BSc. in Computer Science and Engineering

ASSIGNMENT

Course Code: CSE334

Course Title: Pervasive Computing

SUBMITTED TO

Mr. Mohammad Jahangir Alam
Senior Lecturer
Department of CSE
Daffodil International University

SUBMITTED BY

MD Saimim Islam Khan Hamim
ID:212-15-4219

SUBMISSION DATE:29/05/2024

Date: 27.02.23

Leeture Slide I

// Pervasive computing also called ubiquitous computing

Characteristic of PC

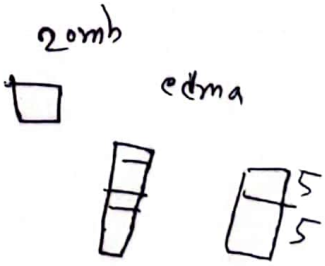
- Physical intregration
- Instantaneous

Leeture Slide II

Handheld computer → personal ~~assistant~~ digital assistant (PDAs).

Palm OS Windows CE

Palm OS
→ Address book
→ Memo Pad (Excel)
→ Date book
→ Mail application



, EPOC is a versatile operating System
- MC218 from Ericsson

GSM (Global Sayten for Mobile Communication

Smart Identification

Smart card:

~~1. Magnetic Strip~~

1. CPU → 8 bit, 5MHz, 5V Optional: crypto coprocessor.

RAM → 4kb

ROM → 16kb
- Operating System
- Communication
- Security (DES, RSA

EEPROM → 16K
- File system
- Program files
- Keys
- Password
- Application

$1 \leq e \leq 12$

2, 3, 4, 5, 6, 7, 8, 9, 10, 11

RSA

① Prime number P, q

② $n = p * q$

③ $\varphi(n) = (p-1) * (q-1)$

④ Public key, e $\quad e = \gcd(\varphi(n), e) = 1, \ 1 < e < \varphi(n)$

⑤ Private key, d, $\quad \frac{ed - 1}{\varphi(n)}$

⑥ encryption

⑦ Decryption

① $P = 3; \ q = 7$

② $n = 21$

③ $\varphi(n) = 2 \times 6 = 12$

④ $e = 5$

⑤ $d = 17$

$c = m^e \bmod n$

$m = c^d \bmod n$

$d = \frac{1 + k\varphi(n)}{e}$

$= \frac{1 + k12}{5}$

$d = \frac{1 + k12}{5}$ (41)

$(n, e) = 1, \quad 1 < e < 12$

$e \times d \bmod \varphi(n) = 1$

$5 \times 17 \bmod 12 = 1$

$85 \bmod 12$

12	13	13/5 =
24	25	25/5 = 5x
36	37	37/5 =
48	49	49/5 =
60	61	
72	73	
84	85	17

Smart Identification

Two types of smart card:

- contact
- contactless

Contact:
The card communicate withe the external devices through a direct physical connection. for example the card is inserted into a terminal. Vending Machine, Goverment IDs, e commerce

Contactless:
The chip communicates with external devices using radio frequency identification (RFI) or radio waves.

- student identification

Smart card components

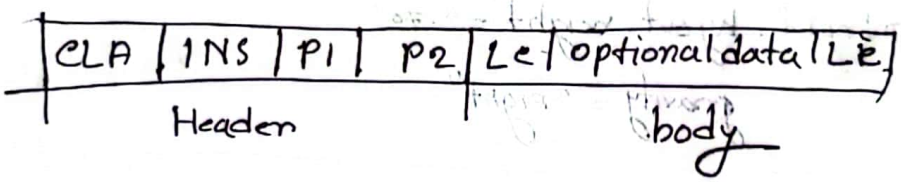
1. CPU
2. RAM
3. ROM
4. EEPORM

APDU (Application Protocol Data Unit)

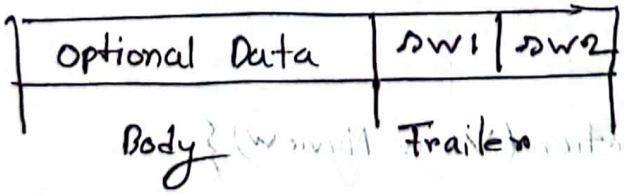
two types:

- Command APDUs (sent from the off-card application to the smart card)
- Response APDUs (sent back from the smart card to reply to commands)

Command APDUs



Response APDUs



Android

android: orientation = "vertical"

android: weightSum = "7"

" Textview

android: id:

android: layout_width = "match_parent"

android: layout_height = "0dp"

android: layout_weight = ".70"

gravity = "right"

For Back button:

android: background = "@drawable/backspace

Public void DigitFunction (View Myview) {

digitbtnobj = findViewById (Myview.getId());

primarydisplayobj

String initialValue = digitbtnobj.getText().toString();

Quiz: 2 9 March

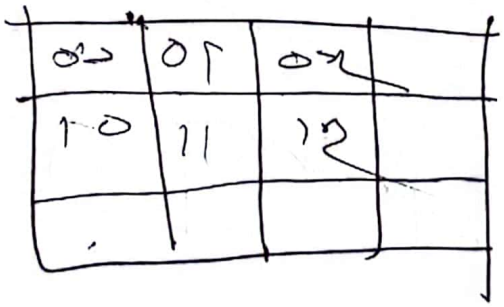
Time: 4.15 PM

Room: 201

Chapter: 4, 5

project presentation 13 March

1. Title
2. Motivation
3. Objective
4. UI
5. Challenge



Mid syllabus:

1. Introduction to pervasive computing
2. Information access devices ✓ .
3. Smart Identification. ✓
4. Embeded controls
5. RSA
6. 5. Security
7. 5. Security.

RSA Algorithm (Rivest-Shamir-Adleman)

RSA algorithm is an asymmetric cryptography algorithm.

two prime number P, Q

C = chipper text

M = Plain text

e = Public key

d = Private key

theory:

$n = p * q$

$\phi(n) = (p-1) \times (q-1)$

$e = \frac{1 + k\,\phi(n)}{d}$

$d = \frac{1 + k \cdot \phi(n)}{e}$

$p = 3;\ q = 7$

$\phi(n) = 2 \times 6$

$= 12$

$e = \frac{1 + k(12)}{d}$

Encryption: $c = m^e \bmod n$

Decryption $m = c^d \bmod n$

Ex 1:

$p = 13, q = 17$

$n = 221$

$\phi(n) = 12 \times 16 = 192$

$e = 35$

$d = 11$

Ex :2

$n = 13 \times 3 = 39$

$\phi n = 12 \times 2 = 24$

$e = 3$

$d =$

$n = 33$

$\phi n = 10 + 2 = 12$

$d = 7$

$e = 3$

12

Enepypting CS

Let,

$P = 7$ and $q = 5$

$n = 35$

$\phi(n) = 24$

$e = 5$

$d = 29$

$c = 3 \quad S = 17$

We know,

cipher text $c = m^e \bmod n$

$= 3^5 \bmod 35$

$= 33$

cipher text $S = 17^5 \bmod 35$

$= 24$

Decryption

We know,

$m = c^d \bmod n$

for c $= 33^{29} \bmod n$

$= ((33^5 \bmod 35) \times (33^5 \bmod 35) \times (33^5 \bmod 35) \times (33^5 \bmod 35) \times (33^5 \bmod 35)) \bmod 35$

$= 16 \bmod 35$

$= 3$

Pervasive comp Lecture 1

Pervasive computer Principles:

- Decentralization
  - Distributed system
  - Synchronizing Information
  - Managing Application.
- Diversification
- Connectivity
- Simplicity
- Targeting specific needs
- Alternatives

Simplified three tire vertical structure:

1. Device
2. Server
3. Work station

Smart Identification

Contact and contactless card:

Contact:
The chip communicates with external devices through a direct physical connection, ~~through~~ the card is inserted into a terminal.

Contactless:
The chip communicates with external devices through a radio wave or RFI connection.

The computer on the smart card:

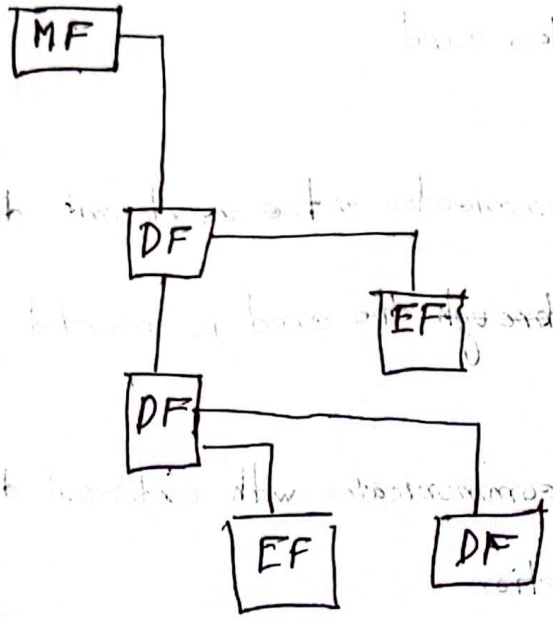
CPU:
- 8 bit
- 5 MHz, 5V
- optional:
  crypto-coprocessor

RAM
- 4kb

ROM (16k)
- Operating system
- communication
- security (RSA, DSA)

EEPORM
- Filesystem
- Program files
- keys
- Passwords
- Applications

File system :



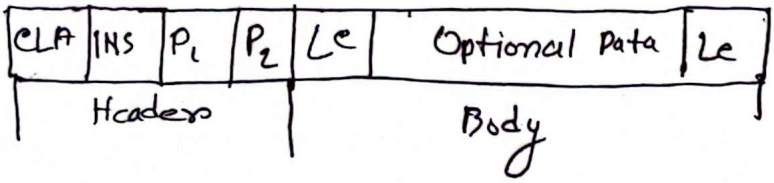
APDUs (Application Protocol Data Unit)s

APDUs are Use to exchange data between host and smart card.

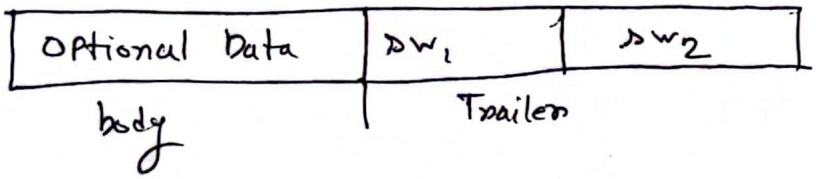
ISO 7816-4 (5099) Defines two types of APDU.

1. Command APDU → off-card application to smart card
2. Response APDU

Command Apdu



Response Apdu



24×1 = 24
2×12 = 24
3×8 = 24
4×6 = 24

RSA

Two large prime numbers:

p & q

$\phi n = (p-1) \times (q-1)$

$e = 1 < e < \phi(n)$ or $\gcd(e, \phi(n)) = 1$

$d = \frac{1 + k\phi(n)}{e}$

e if the eq

e Cipher text $c = m^e \bmod n$

Plain text $m = c^d \bmod n$

Question,

Given,

$e = 11,937$

$d = 187$

$d = \frac{1 + k \times \phi(n)}{e}$

$11 \times 187 \bmod \phi(n) = 1$

$\Rightarrow 187 \times 11 \bmod (p-1)(q-1)$

$\Rightarrow 2057 = 1 \pmod{(p-1)(q-1)}$

2057

mod 2057

Let,

two prime number,

$p = 5;\ q = 7$ ⟸ 3, 5, 7, 11, 13

$n = 35$

$\phi(n) = 4 \times 6 = 24$

$e = 5$

$d = \frac{1 + k(\phi(n))}{e}$

24	24+1=25	25/5=5 ✓
48	48+1=49	true
72	72+1=73	true
96	97	true
120	121	true
144	~~145~~ 145	29

$d = 29$

given message = 3, 19

we know,
$e = 3$; $S = 19$

Now,
chiffen text $c_{(3)} = M^e \bmod n$
$= 3^5 \bmod 35$
$= 33$

chiffen text $c_{(19)} = 19^5 \bmod 35$
$= 24$

243 K/C

Now,
plain text $M = c^d \bmod n$
$= 33^{29} \bmod 35$
$= ((33^5 \bmod 35)(33^5 \bmod 35)(33^5 \bmod 35)(33^5 \bmod 35)$
$(33^5 \bmod 35)(33^4 \bmod 35) \bmod 35)$
$= 3$ A