

Assignment 6

Zhanserik Gaziz

Task 1 — Polybius Square method

D	X	E	M	U
R	L	B	Y	N
A	Z	K	F	V
W	G	O	S	C
Q	I,J	T	H	P

ORGANIZED CRIME → TAIWVZLBR PAZYB

Task 2 — Caesar Cipher

Text: OPERATING SYSTEMS

Key: K = 3

ABCDEFGHIJKLMNOPQRSTUVWXYZ

OPERATING SYSTEMS → RSHUDWLQJ VBWHPV

Task 3 — Trisemus Method

Text: SCREEN

Key: TYPE

TYPEA

BCDFG

HIKLM

NOQRS

UVWXZ

SCREEN → ZIXFFU

Task 4 Program

```
1 usage
function caesarEncryptDebug($text, $key, &$log) {
    $result = "";
    for ($i = 0; $i < strlen($text); $i++) {
        $char = $text[$i];
        if (ctype_alpha($char)) {
            $base = ctype_lower($char) ? ord( character: 'a') : ord( character: 'A');
            $oldPos = ord($char) - $base;
            $newPos = ($oldPos + $key) % 26;
            $newChar = chr( codepoint: $newPos + $base);
            $log .= "Encrypt: $char ($oldPos) + $key → $newChar ($newPos)\n";
            $result .= $newChar;
        } else {
            $result .= $char;
        }
    }
    return $result;
}
```

```
1 usage
function caesarDecryptDebug($text, $key, &$log) {
    $result = "";
    for ($i = 0; $i < strlen($text); $i++) {
        $char = $text[$i];
        if (ctype_alpha($char)) {
            $base = ctype_lower($char) ? ord( character: 'a') : ord( character: 'A');
            $oldPos = ord($char) - $base;
            $newPos = ($oldPos - $key + 26) % 26;
            $newChar = chr( codepoint: $newPos + $base);
            $log .= "Decrypt: $char ($oldPos) - $key → $newChar ($newPos)\n";
            $result .= $newChar;
        } else {
            $result .= $char;
        }
    }
    return $result;
}
```

Caesar Cipher

Text

Key (K)

Encrypt

Encrypted result

Decrypt

Process

Encrypt: $P = (14) + 1 = P = (15)$

Caesar Cipher

Text

Key (K)

Encrypt

Encrypted result

Decrypt

Decrypted result

Task 5

Caesar



unsaved001.txt

*unsaved002.txt X

*out001.txt

Hello world!



kmars

JCryptTool 1.0.9

unsaved001.txt

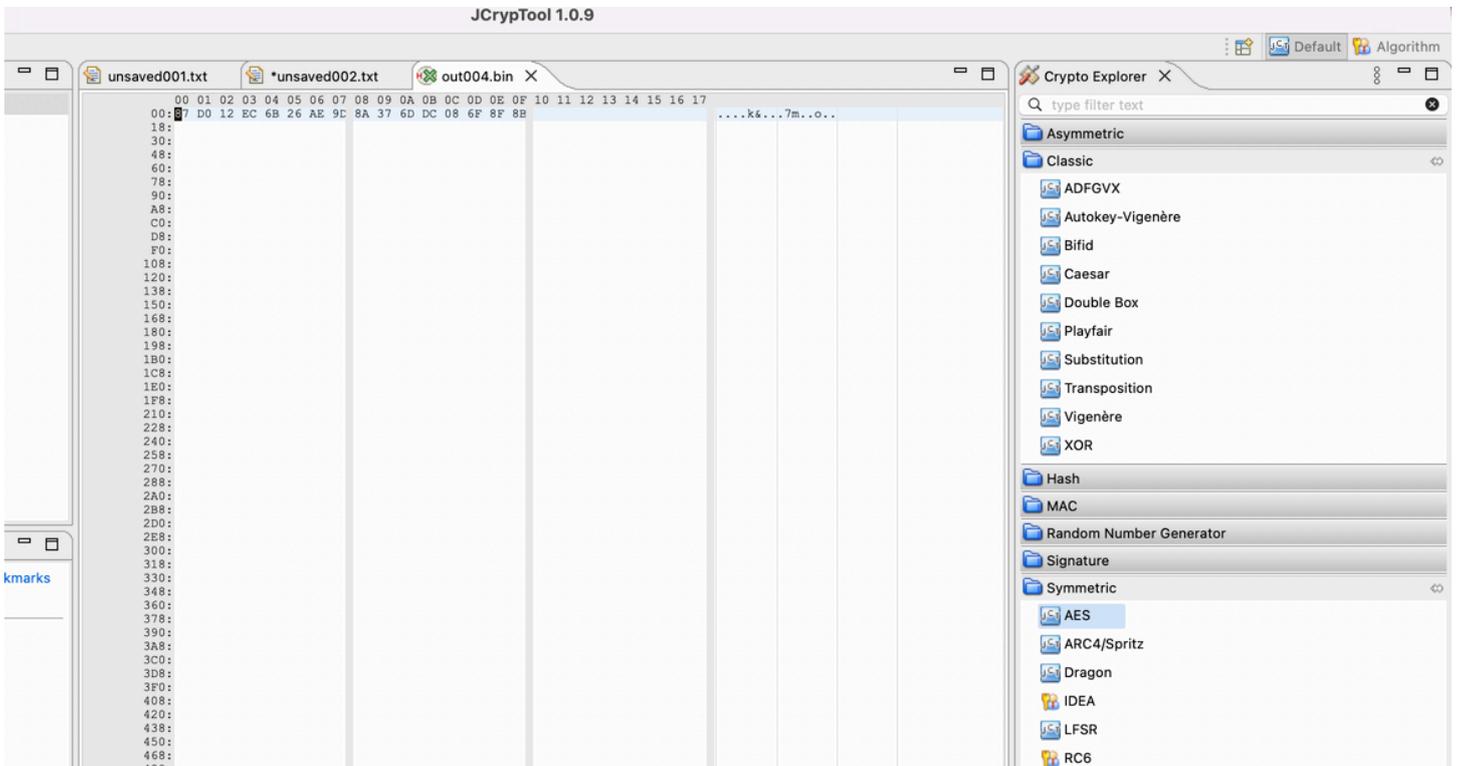
*unsaved002.txt

*out001.txt X

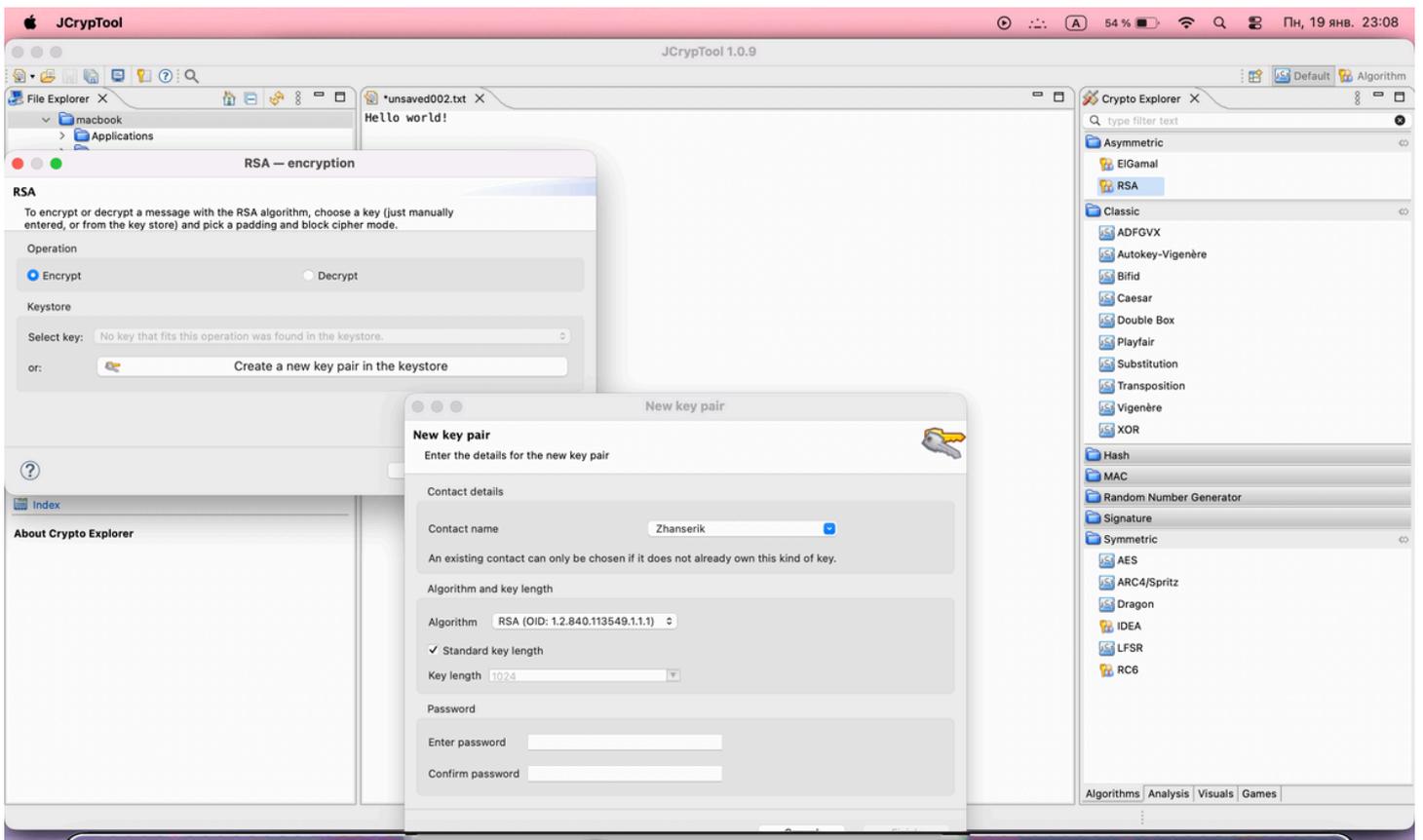
JGNNQ YQTNF!

arks

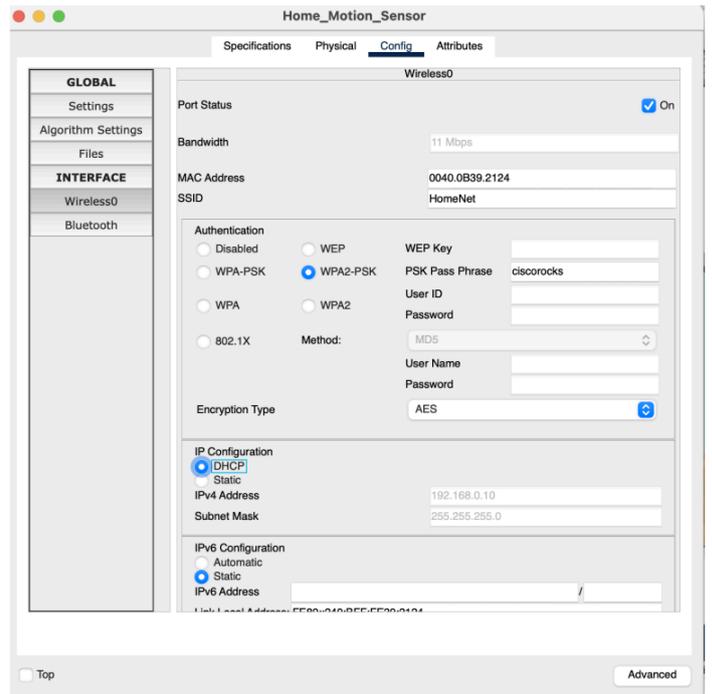
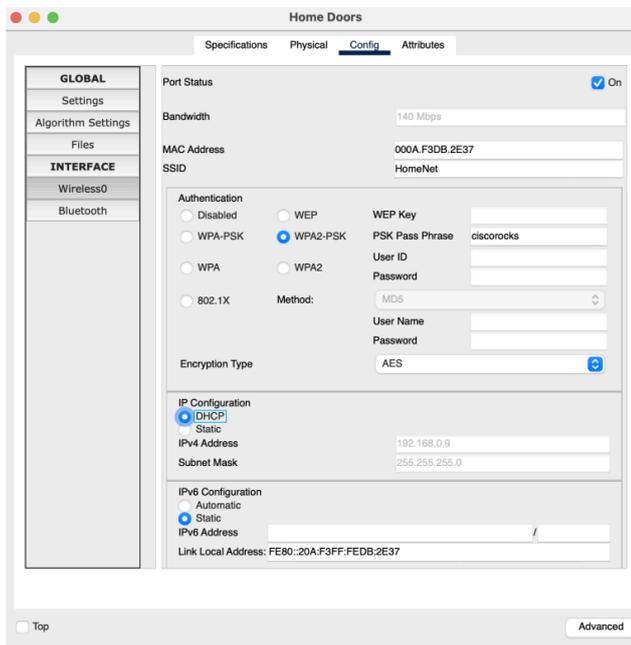
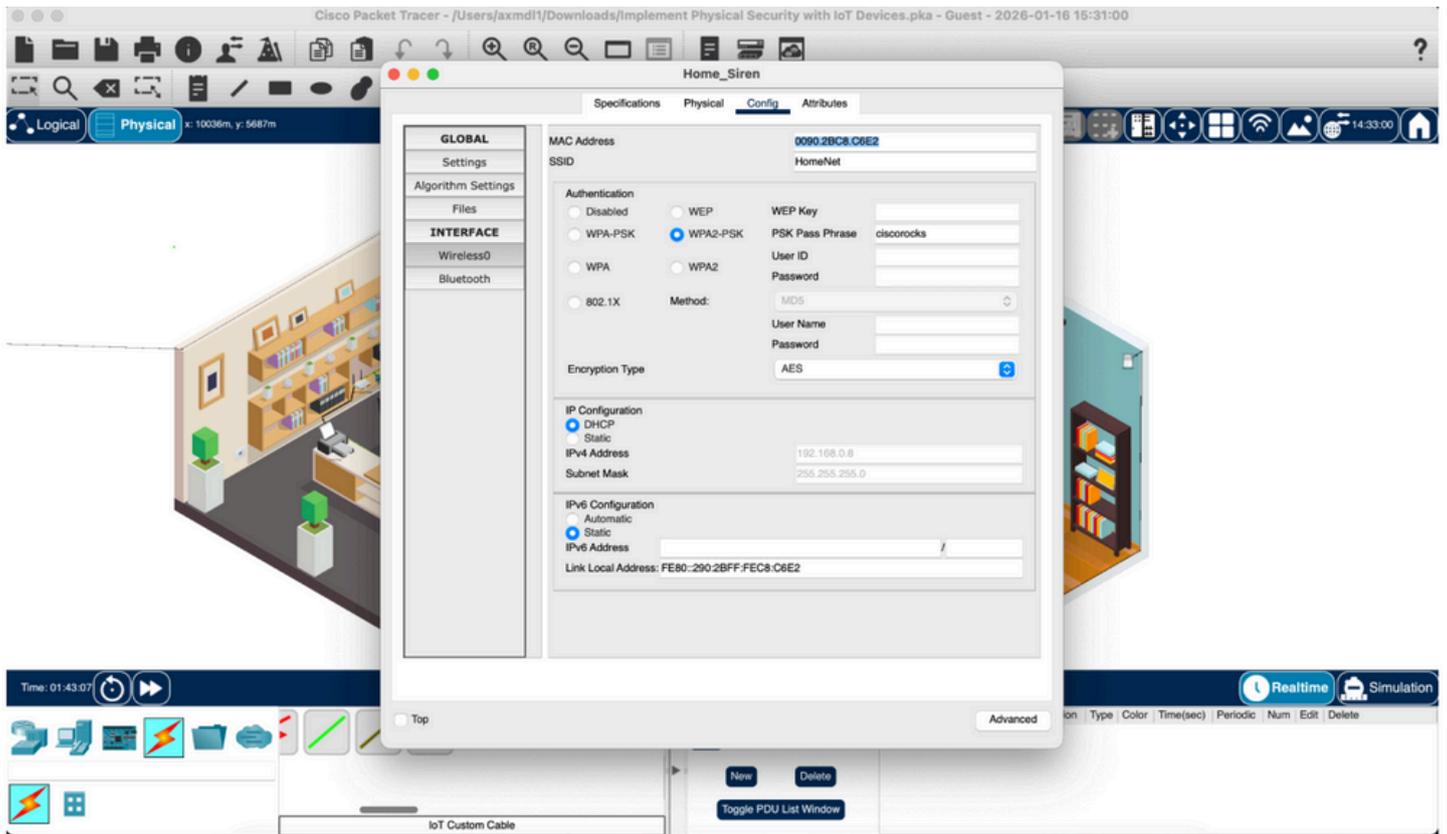
AES



RSA



Packet Tracer



Home_Webcam

Specifications Physical **Config** Attributes

GLOBAL

- Settings
- Algorithm Settings
- Files

INTERFACE

- Wireless0
- Bluetooth

Wireless0

Port Status On

Bandwidth 300 Mbps

MAC Address 00D0.58D1.C411

SSID HomeNet

Authentication

- Disabled
- WEP
- WPA-PSK
- WPA2-PSK
- WPA
- WPA2
- 802.1X

WEP Key

PSK Pass Phrase ciscorocks

User ID

Password

Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

- DHCP
- Static

IPv4 Address 192.168.0.11

Subnet Mask 255.255.255.0

IPv6 Configuration

- Automatic
- Static

IPv6 Address

Link Local Address FE80:2E0:A3FF:FE4E:262B

Top Advanced

Home Office PC

Physical Config **Desktop** Programming Attributes

Web Browser

URL http://192.168.0.1/Wireless_MAC.asp

Go Stop

Wireless Port: 2.4G

Enabled Disabled

Access Resolution

- Prevent PCs listed below from accessing the wireless network
- Permit PCs listed below to access wireless network

Wireless Client List

MAC Address filter list	MAC Address	MAC Address	MAC Address
MAC 01:	00:01:96:36:CE:4C	MAC 26:	00:00:00:00:00:00
MAC 02:	00:90:2B:2C:CB:0D	MAC 27:	00:00:00:00:00:00
MAC 03:	00:E0:F7:6E:B5:CA	MAC 28:	00:00:00:00:00:00
MAC 04:	00:90:2B:C8:C6:E2	MAC 29:	00:00:00:00:00:00
MAC 05:	00:0A:F3:DB:2E:37	MAC 30:	00:00:00:00:00:00
MAC 06:	00:40:0B:39:21:24	MAC 31:	00:00:00:00:00:00
MAC 07:	00:D0:58:D1:C4:11	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 37:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00

Top

Home Office PC

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

- DHCP Static DHCP request successful.

IPv4 Address 192.168.0.9

Subnet Mask 255.255.255.0

Default Gateway 192.168.0.1

DNS Server 10.2.0.125

IPv6 Configuration

- Automatic Static ipv6 request failed.

IPv6 Address

Link Local Address FE80::2E0:A3FF:FE4E:262B

Default Gateway

DNS Server

802.1X

- Use 802.1X Security

Authentication MD5

Username

Password

Top

Home_Siren

Specifications Physical **Config** Attributes

GLOBAL

- Settings
- Algorithm Settings
- Files

INTERFACE

- Wireless0
- Bluetooth

Interfaces Wireless0

Gateway/DNS IPv4

- DHCP Static

Default Gateway 192.168.0.1

DNS Server 10.2.0.125

Gateway/DNS IPv6

- Automatic Static

Default Gateway

DNS Server

IoT Server

- None
- Home Gateway
- Remote Server

Server Address 10.3.0.125

User Name HomeUser

Password Pa\$\$w0rd

Refresh

Top Advanced

Home Doors

Specifications Physical **Config** Attributes

GLOBAL

Settings

Algorithm Settings

Files

INTERFACE

Wireless0

Bluetooth

Default Gateway: 192.168.0.1

DNS Server: 10.2.0.125

Gateway/DNS IPv6

Automatic

Static

Default Gateway: _____

DNS Server: _____

IoT Server

None

Home Gateway

Remote Server

Server Address: 10.3.0.125

User Name: HomeUser

Password: Pa\$\$w0rd

Refresh

Device Clock: 13:00:35 Mon Mar 1 1993 UTC

NTP

Server Ip: _____

Authentication

Top Advanced

Home_Motion_Sensor

Specifications Physical **Config** Attributes

GLOBAL

Settings

Algorithm Settings

Files

INTERFACE

Wireless0

Bluetooth

Interfaces: Wireless0

Gateway/DNS IPv4

DHCP

Static

Default Gateway: 192.168.0.1

DNS Server: 10.2.0.125

Gateway/DNS IPv6

Automatic

Static

Default Gateway: _____

DNS Server: _____

IoT Server

None

Home Gateway

Remote Server

Server Address: 10.3.0.125

User Name: HomeUser

Password: Pa\$\$w0rd

Refresh

Home_Webcam

Specifications Physical **Config** Attributes

GLOBAL

Settings

Algorithm Settings

Files

INTERFACE

Wireless0

Bluetooth

Interfaces: Wireless0

Gateway/DNS IPv4

DHCP

Static

Default Gateway: 192.168.0.1

DNS Server: 10.2.0.125

Gateway/DNS IPv6

Automatic

Static

Default Gateway: _____

DNS Server: _____

IoT Server

None

Home Gateway

Remote Server

Server Address: 10.3.0.125

User Name: HomeUser

Password: Pa\$\$w0rd

Refresh

Home Office PC

Physical **Config** Desktop Programming Attributes

Web Browser

URL: http://10.3.0.125/home.html

IoT Server - Devices Home | Conditions | Editor | Log Out

- ▶ Home_Siren (PTT0810QD31-) Siren
- ▶ Home_Doors (PTT0810G94Z-) Window
- ▶ Home_Motion_Sensor (PTT081016MF-) Motion Detector
- ▶ Home_Webcam (PTT0810T8HX-) Webcam

Home Office PC

Physical Config **Desktop** Programming Attributes

IoT Server - Devices Home | Conditions | Editor | Log Out

- ▶ Home_Siren (PTT0810QD31-) Siren
- On [Red Stop Button]
- ▶ Home_Doors (PTT0810G94Z-) Window
- On [Red Stop Button]
- ▶ Home_Motion_Sensor (PTT081016MF-) Motion Detector
- On [Red Stop Button]
- ▶ Home_Webcam (PTT0810T8HX-) Webcam
- On [Red Stop Button]
- Image [Green Start Button]

