ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Homework Assignment - Crypto

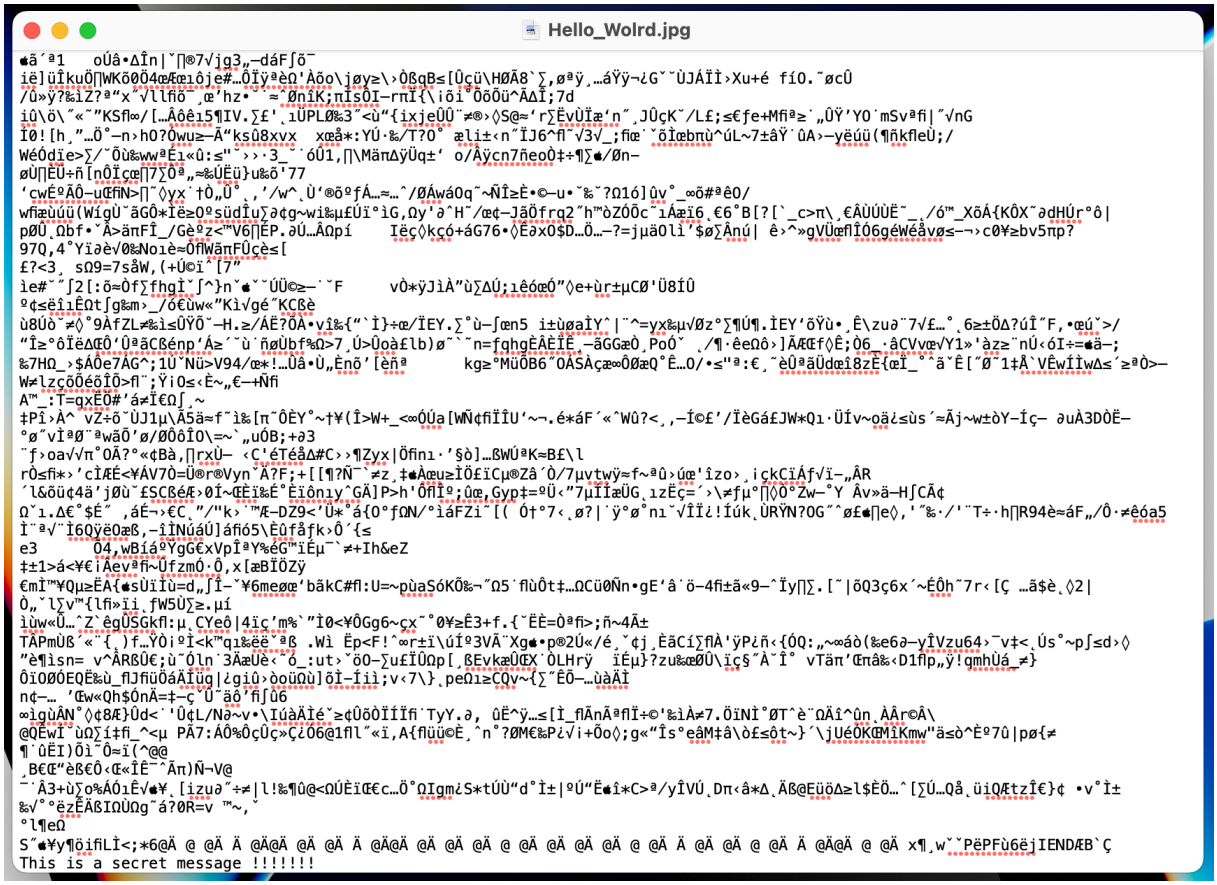
Cyber Security and Resilience Program

Flita-Vasile Adrian

1 Hide a text of your choice in an image. Attach the image to the assignment. Make a screenshot of the source code of the image and show the occurence of the text. Why is it possible to hide data inside an image?

1.1 Solving:

The method I used for hiding a text into an image is opening the image using a text editor, then scrolling down towards the end of it's binary code and simply add the secret messsage. In this way the image is not modified and you would not see any difference while opening it with an image viewer.



So hiding a text into an image is a basic principle of Steganography, which is hiding data in creative ways. "Sometimes the best way to share sensitive information is to hide it in plain sight". It is useful if you want to send an encrypted message without raising any suspicion.

2 Encrypt the sentence ”This is Vigenere encrypted” (without the quotes) with a password of your choice using the Vigenere algorithm. Write down the ciphertext and the password.

2.1 Solving:

The meeting is taking place at 12PM at the secret office - The message we want to encrypt

”car”- the key

Vhv oevviei ij vabknx rlree rv 12PD ct kje jgcigt fhfzee - Encrypted message

3 Encrypt the following sentence using AES: ”buy me some potato chips please”. Use the key ”keys are boring1”. Encrypting the first block is sufficient. If you want to do the second block as well, pay attention to the padding! Write down any steps you do and any intermediate results. (Duckduckgo is your friend.)

3.1 Solving:

Both software and hardware are efficient with AES, which uses a substitution–permutation network design principle.

AES OPERATES on a 4x4 column-major order array of bytes. For that to be possible you take the first 16 bytes of the message you want to encrypt.For the process of encryption it is also needed a key. The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

1. KeyExpansion

2. Initial round key addition:

2.1.Add Round key

2.2.SubBytes- a non-linear substitution where is byte is replaced using AES S-box

2.3.ShiftRows

2.4.MixColumns

2.5.AddRoundKey

3.Final round (making 10,12,or 14 rounds in total):

3.1.SubBytes

3.2.ShiftRows

3.3.AddRoundKey

Rest of the solving is attached down to the document

Side note: for the message that needs be encrypted I have not taken the spaces into consideration

4 Generate a RSA key pair of your choice. Mark your private and public key. Encrypt "This is secret" and decrypt it afterwards. Write down any steps you do and any intermediate results.

4.1 Solving:

First we select two random prime number:p=11 and q=5.

2.N=p*q=55.

Phi(N)=(p-1)*(q-1):40.

3.Selecting Value for public e. e must be smaller than Phi(n), and is coprime to Phi(n).

e=7.

4.Calculating d using the following equation d(e)=1 mod Phi(n). In our case is d(7)=1 mod 40. d=23.

"This is secret"-The message we need to encrypt.

For encryption we look at the ASCII table for each letter and use the formula: $(m^e)mod$ n.

Our message in ASCII: **084 104 105 115 032 105 115 032 115 101 099 114 101 116**

Encrypted message:39,14,30,25,43,30,25,43,25,51,44,49,51,41

Decrypted message:29,49,50,5,32,50,5,32,5,46,44,4,46,6

5 Read about the structure of the European eID structure. What is the speciality in the architecture of the various countries and their trust relationship regarding PKI and Web-of-Trust principles? What may be the reason for this architecture?

5.1 Solving:

As part of the DIGITAL eID building block, the European Commission provides a set of services (software, documentation, training, and support) endorsed by the Member States, enabling public administrations and private service providers to offer online services to citizens from other European countries. The system achieves this by mutually recognising national electronic identification (eID) schemes (such as smartcards, mobile and login) so that citizens can securely access online services provided in other European countries using their national eIDs.The system achieves this by mutually recognising national electronic identification (eID) schemes (such as smartcards, mobile and login) so that citizens can securely access online services provided in other European countries using their national eIDs.

A public key cryptography method requires a Public Key Infrastructure (PKI), which consists of the policies, practices, and technology required to maintain digital certificates. A digital certificate is an electronic data structure that links a particular entity to its public key, such as an organization, a person, a computer program, a web address, etc. Public key cryptography and digital signatures are used in conjunction with digital certificates to facilitate secure communication. To ensure that the certificate can be trusted, a PKI is used.

Trust is the main goal of a public key cryptography system. A digital certificate is an electronic signature that verifies the authenticity and validity of a public key and comes from one or more vetted third parties. Similar to how passports serve as identity proof for citizens, this certificate serves as the digital identifying proof that verifies an entity is who it claims to be. There are two trust models that are utilized in practice: central ”Certification Authority” based and ”Web of Trust.”

For many countries ”Web of Trust” is the perfect choice when it comes to trust models. When certified entities are humans, the ”Web of Trust” system is applicable. In this instance, individuals can physically sign the certificates of other persons they directly know or whose identification they have confirmed through formal documentation. People can select their own personal trust thresholds based on the trust relations graph that is produced as a result of this.

One of the main reason for choosing this model is its theoretical simplicity and resistance to compromise by any one participant. One of its downsides that might be taken into consideration its dependency on people following the right procedures and lack of a dedicated central management makes cataloguing and especially the revocation of certificates complicated.

PROBLEM 3

1st BLOCK

$$\begin{bmatrix} B & E & E & A \\ U & S & P & T \\ Y & O & O & O \\ M & M & T & C \end{bmatrix} \longrightarrow \begin{bmatrix} 42 & 45 & 45 & 41 \\ 55 & 53 & 50 & 54 \\ 59 & 4F & 4F & 4F \\ 4D & 4D & 54 & 43 \end{bmatrix}$$

SubBytes with S-BOX

$$\rightarrow \begin{bmatrix} 36 & 20 & 20 & FA \\ FC & 96 & 6B & 6E \\ 2A & BF & BF & BF \\ 03 & 48 & 6E & 18 \end{bmatrix} \text{SHIFT} \begin{bmatrix} 36 & 20 & 20 & FA \\ 96 & 6B & 6E & FC \\ BF & BF & 2A & BF \\ 18 & 03 & 48 & 6E \\ A & B & C & D \end{bmatrix}$$

MIX COLUMS

$$Q_{A1} = 2 \cdot 36 \oplus 3 \cdot 96 \oplus BF \oplus 18 = \underline{109}$$

$$Q_{A2} = 36 \oplus 2 \cdot 96 \oplus 3 \cdot BF \oplus 18 = \underline{33F}$$

$$Q_{A3} = 36 \oplus 96 \oplus 2 \cdot BF \oplus 3 \cdot 18 = \underline{196}$$

$$Q_{A4} = 3 \cdot 36 \oplus 96 \oplus BF \oplus 2 \cdot 18 = \underline{BB}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

FIXED MATRIX

$Q_{B1} = 2 \cdot 20 \oplus 3 \cdot 6B \oplus BF \oplus 03 = \underline{1BD}$

$Q_{B2} = 20 \oplus 2 \cdot 6B \oplus 3 \cdot BF \oplus 03 = \underline{2C8}$

$Q_{B3} = 20 \oplus 6B \oplus 2 \cdot BF \oplus 3 \cdot 03 = \underline{13C}$

$Q_{B4} = 3 \cdot 20 \oplus 6 \cdot B \oplus BF \oplus 2 \cdot 03 = \underline{B2}$

$Q_{C1} = 2 \cdot 20 \oplus 3 \cdot 6E \oplus 2A \oplus 48 = \underline{168}$

$Q_{C2} = 20 \oplus 2 \cdot 6E \oplus 3 \cdot 2A \oplus 48 = \underline{CA}$

$Q_{C3} = 20 \oplus 6E \oplus 2 \cdot 2A \oplus 3 \cdot 48 = \underline{C2}$

$Q_{C4} = 3 \cdot 20 \oplus 6E \oplus 2A \oplus 48 = \underline{B4}$

$Q_{D1} = 2 \cdot FA \oplus 3 \cdot FC \oplus BF \oplus 6E = \underline{3D1}$

$Q_{D2} = FA \oplus FC \oplus 3BF \oplus 6E = \underline{351}$

$Q_{D3} = FA \oplus FC \oplus 2 \cdot BF \oplus 3 \cdot 6E = \underline{32}$

$Q_{D4} = 3 \cdot FA \oplus FC \oplus BF \oplus 2 \cdot 6E = \underline{271}$

'RESULT OF MIX COLUMS 1

$$\begin{bmatrix} 109 & 1BD & 168 & 3D1 \\ 33F & 2C8 & CA & 351 \\ 196 & 13C & C2 & 32 \\ BB & B2 & B4 & 271 \end{bmatrix}$$

KEY BLOCK

$$\begin{bmatrix} K & & & I \\ E & A & B & N \\ Y & R & O & G \\ S & E & R & 1 \end{bmatrix} \xrightarrow{HEX} \begin{bmatrix} 4B & 20 & 20 & 49 \\ 45 & 41 & 42 & 4E \\ 59 & 52 & 4F & 47 \\ 53 & 45 & 52 & 31 \end{bmatrix}$$

$$= \begin{bmatrix} 142 & 19D & 148 & 398 \\ 3FA & 289 & 88 & 31F \\ 1CF & 16E & 8D & F5 \\ E8 & FF & E6 & 240 \end{bmatrix}$$