ART

Digital Portraits Service Web App

Nolasco Cid Víctor Iván : Co-creator

What is ART?

ART is a **web application** which provides a secure platform for the service of digital portraits.

Users pay painters to make **digital portraits** from their photos.

The users can send their photos through the Internet, after a few weeks the painters will create portraits from these photos and send them to users.

What does ART offer?

ART offers the following cryptographic services: Privacy, Authentication, Integrity, Non Repudiation.

For art lovers

- All the communication is encrypted
- Your photos will be stored encrypted
- Authenticity guarantee on paintings

For artist

- Secure channel of communication
- Clients authentication
- Clients can’t deny orders

Status of ART

ART is a school project that I developed together with my classmates Mayra Hernandez Oseguera and Eric Lopez Ayala for my **Cryptography** class at ESCOM.

It was developed from April to June 2019.

My participation

The role I played in the development of **ART** was as a backend security developer. I developed all the security in the backend with **Python3** using the **Pycryptodome** library.

To guarantee that ART offers the previously described cryptographic services, I used **cryptographic primitives** such as **AES ciphers**, **HASH functions**, **RSA Digital Signature** schemes, among others.

I also made use of the **PyArmor** tool, for **obfuscating** files on the server and providing extra security.

Code Example for images encryption with AES

```
def encrypt_image(id, image_file_name, directory):
    """encrypt and store the client photo"""
    image_bytes = get_image_bytes(image_file_name)
    o_key = readBinFile(BASE_DIR +'\\CryptoProject\\keys\\orders\\' + str(id) + '_key.bin')
    key = decrypt_key(o_key)
    iv = readBinFile(BASE_DIR +'\\CryptoProject\\keys\\orders\\' + str(id) + '_iv.bin')
    #build an AES cipher using OFB mode
    cipher = AES.new(key, AES.MODE_OFB, iv)
    #encrypt the images bytes
    cipher_image_bytes = cipher.encrypt(image_bytes)
    writeBinFile(cipher_image_bytes, BASE_DIR +
'\\CryptoProject\\app\\static\\images\\'+directory+'\\' + str(id) + '.bin')
```

More about ART

For more information about **ART** consult the documentation in the following link: [ART Documentation]

It contains images and descriptions about its operation, and a better explanation about the **architecture** of the application, the **security** and the **technologies** with which it was developed.

Check all the source code in the following Github repository:

https://github.com/escomcrypto/Crypto2019