UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI
1818

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea Calculatoarelor și a Rețelelor

26. Aplicarea algoritmilor criptografici asimetrici

Cryptography

Tasks

1. [2p] There are several tools used for hiding files behind an image. Create a file “Lab08.txt” and add the following line: “Thanks GOD that this lab is NOT part of the exam.” Use `jphide.exe` and `jpseek.exe` to hide this info behind a JPG file. (http://images.google.com/ fileype:jpg)
2. [+1p=3p] Archive the jphide.exe file into a .7z file using the 7zip utility already installed. Combine the image you’ve previously downloaded with this file using the copy.exe command in cmd. Make it a binary copy of those to files into a new .jpg file. What is the size of the new file? How can you reveal the archive created?
3. [+1p=4p] Write in a notepad your name using the Caesar cipher. The key is equal to the number of letter in your name. (use both first and last names)
4. [+2=6p] You have to use the following algorithm to decrypt the message “08324F5C”.

```
const char *xlat = "dsfd;kfoA,.iyewrkldJKDHSUBsgvca69834ncxv";

char *unseven(const char *hash)
{
    unsigned int key, i, hlen = strlen(hash) - 2;
    char *plain = (char*)malloc(hlen / 2 + 1);

    if (hlen < 2 || hlen & 1) return NULL;

    key = (hash[0] - '0') * 10 + hash[1] - '0';
    if (key > 15 || !isdigit(hash[0]) || !isdigit(hash[1])) return NULL;

    hash += 2;
    for (i = 0; i < hlen; ++i) if (!isxdigit(hash[i])) return NULL;

    for (i = 0; i < hlen; i += 2) {
        plain[i / 2] = ((hex2int(hash[i]) << 4) | hex2int(hash[i + 1])) ^ xlat[key++];
        if (key == 40) key = 0;
    }
    plain[hlen / 2] = 0;

    return plain;
}
```

    a. Hint: http://www.asciitable.com/
    b. Hint: http://www.cprogramming.com/tutorial/bitwise_operators.html

5. [+1=7p] Try to access the picture file from the USB. Now, import the certificate from the archive to your local computer. Try again.
6. [+1=8p] Generate a certificate using the cipher.exe utility from Windows cmd. Encrypt one of you local directories (C:\Facultate\SCR). Now switch to another user (e.g.: PR) and try to access that directory.
    a. Hint: http://technet.microsoft.com/en-us/library/bb457065.aspx#EHAA
7. [+1=9p] Create a certificate for the previously user (PR) and make sure that this user can also access the file, only two users can access the file.
8. [+2=11p] Encryption contest. Create a symmetric encryption algorithm that uses substitution/transposition method applied directly on a block. Start!

Interesting fact: the algorithm from point five is used for type 7 decryption in Cisco IOS.