

Introduction to MD5

CS681 & CS392 Computer Security

Fall 2004

Due 10/06/2004

September 30, 2004

1 Objective

The objectives of this assignment are 1) Implement the extended file encryption mechanism you designed in the previous lab and 2) Design and implement file signing and verification features for FEAU using MD5.

2 MD5

You should be familiar with the MD5 algorithm. This was covered extensively in class this week.

- You can learn more about MD5 from: <http://www.freesoft.org/CIE/RFC/1321/3.htm>
- Use the MD5 code that came with RSA code that you used in the previous lab.
- Get familiarized with MD5 sample code.

2.1 Warm Up

Answer the following questions:

1. Name three popular hash functions used today, give a brief (three line at most) description for each.
2. What does MD5 stand for?
3. Who developed MD5 algorithm and when?
4. What was the initial motive for the development of MD5?
5. You have learnt that a good cryptographic function can also work as a hash function, so can a hash function be used for encryption and decryption? if so, explain.
6. What would be the advantages and disadvantages for doing the above? Explain in terms of local laws, computational complexity, and cryptographic strength.

2.2 Implementing Extended File Encryption

Here is a simple mechanism to solve the problem presented to you in the previous assignment.

- Uk_{pub} = User's Public Key
- Uk_{prv} = User's Private Key
- fk_s = AES file encryption Key
- Gk_{pub} = Group Public Key
- Gk_{prv} = Group Private Key

- Ak_{pub} = Administrative group's Public Key
- Ak_{prv} = Administrative group's Private Key

File encryption and decryption process:

1. Generate a n bit random number and use it as fk_s . n is equal to the size of the AES key in use (128, 192, or 256).
2. Encrypt the file F using AES: $E_{fk_s}(F)$
3. Encrypt fk_s using public key of the user, administrative group, other user's or group's allowed, and concatenate it the encrypted file $E_{fk_s}(F)$: $E_{fk_s}(F) || mark || E_{Uk_{pub}}(fk_s) || E_{Ak_{pub}}(fk_s) || E_{Gk_{pub}}(fk_s) || mark$. $mark$ is a constant string that is being used as preamble and post-amble.
4. To decryption is a given file a user simply have to decrypt the corresponding $E_{Uk_{pub}}(fk_s)$ to get the AES encryption key fk_s and decrypt the file: $D_{Uk_{prv}}(E_{Uk_{pub}}(fk_s)), D_{fk_s}(F)$.

For this section you should integrate your extended file encryption mechanism into FEAU. You could use the above mechanism if yours does not work. As of now enc and dec does not have the capability to distinguish between users so just pass the user name as parameter in enc or dec command. You should pre-compute private key and public key pairs for your users and groups.

2.3 File Signing and Verification

Design and implement the file signing and sign verification commands using MD5. Please note: a user should be able to sign both encrypted and non-encrypted files.

snfl - Sign files

Synopsis - snfl [file...]

Description snfl signs both encrypted and plain file with current users private key.

vfy - Verify file integrity

Synopsis - vfy [files...]

Description vfy check file integrity.

You must document and submit your design and the code for the above commands.

3 What and how to Handin

For this assignment you must submit answers for all of the above section on or before midnight 10/06/2004. We prefer you to e-mail your submission to **graderSecurity@gmail.com** with subject line "lab 3 <your name>" with out the quotes. Subject line is very important if you want to receive any credits.