CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

# Homework #8

Due December 31, 2012, midnight

Please kindly send a PGP encrypted & authenticated e-mail to your instructor. You can obtain your instructor's public key from the course webpage.

You can find plenty of documentation on the Internet about how to operate PGP with your favorite mail client. On our CS domain's `homes` server, GPG 1.4.10 is installed at /opt/csw/bin/gpg. Please make sure that the PGP message you send is compatible with GPG 1.4.10. Most importantly, GPG does not support IDEA. The list of supported algorithms is as follows:

Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2

Also remember to tell your instructor where to find your PGP public key. (Don't ever send your public key over e-mail!)

Some common mistakes experienced in the previous years are as follows:

- Sending your public key over e-mail.
- Sending your message from an address different from the one you generated your public key for.
- Writing your message into a file, encrypting the file with PGP, and then sending it as an attachment.[1]
- Using a machine/software which adds the current host name to the sender's address—so the "From" address in the mail does not match the address in the PGP key.

To avoid these and other potential problems, experimenting with PGP with your friends before sending your homework message is recommended.

Have a happy and peaceful new year. I hope you will find the material you learned in the class useful in your later life as well.

[1] Although PGP can be used for file encryption as well, this is not the proper way to use it for email security.