CS 470
Introduction to Applied Cryptography
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Homework #3
Due April 19, 2013, midnight

Please kindly send a PGP encrypted & authenticated e-mail to your TA (at `mustafa.battal@cs.bilkent.edu.tr`). You can find TA's public key on `http://www.cs.bilkent.edu.tr/~mustafa.battal/public.asc`.

You can find plenty of documentation on the Internet about how to operate PGP with your favorite mail client. Please make sure that the PGP message you send is using widely used algorithms. For example, 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 TA where to find your PGP public key. Dont ever send your public key over e-mail! Suggested method is to submit and verify your key at `http://keyserver.pgp.com/`.

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 senders 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.

To make things more fun, you can try and look for possible witty email contents. (i.e. Bruce Schneier facts)

Enjoy the rest of the semester and I hope you will find the material of this course to be useful.

---

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