Cryptology
Problems

To be discussed Wednesday, March 7, 2001, starting at 8:15 and ending no later than 9:30.

1. First, we will discuss the problems from the first assignment.

2. Review the proof that encrypting a message with a public RSA key and then decrypting with the corresponding private key yields the original message.

3. Look at problems 4.1, 4.2, and 4.3 in the textbook, plus the problem listed below. If you are at all unsure of how to do them, please do them. Even if you are not unsure, you might consider this an opportunity to try using Maple (which is even more useful for problem 4.4 above). The following Maple functions should be useful: `igcdex` (extended Euclidean algorithm for integers), `mod` (where the operation `&^` should be used for more efficient modular exponentiation - try them both to compare), `msolve` (solve equations in $\mathbb{Z}_m$), and `chrem` (Chinese Remainder Algorithm).

4. Another easy problem. Let $n = 143$ be a modulus for use in RSA. Choose a public encryption exponent e and a private decryption exponent d which can be used with this modulus. Try encrypting and decrypting some value to see that the exponents you have chosen work.

KANDIDATSYMPOSIUM OG MATALOGIFEST

Det er ved at være tid til at alle ansatte og studerende mdes til fest, god mad, våde varer og masser af godt humør. Den næste Matalogifest bliver

lørdag d. 31. marts kl 18:45.

Kom og vær med!

Om eftermiddagen holder vi kandidatsymposium med deltagelse af forhbentlig rigtig mange af instituttets tidligere studerende, som ogs er inviteret med til Matalogifesten. Det foregr kl 13–18 i U45. Se programmet for eftermiddagens arrangement p opslagstavlerne.

Festudvalget