**PUBLIC KEY CRYPTOGRAPHY**

# Seminar 5

**1.** Use the 27-letter alphabet from the course (_ABC...XYZ with numerical equivalents 0,1,...,26) for RSA encryption and decryption. Plaintext message units are blocks of $k = 2$ letters, while ciphertext message units are blocks of $l = 3$ letters. The public key is $(n, e) = (1643, 7)$.

(i) Encrypt the plaintexts "Math" and "Info".

(ii) Compute the decryption key $d = e^{-1} \bmod \varphi(n)$, knowing that $n = 31 \cdot 53$.

(iii) Decrypt the ciphertexts.

**2.** Use the 27-letter alphabet from the course (_ABC...XYZ with numerical equivalents 0,1,...,26) for Rabin encryption and decryption. Plaintext message units are blocks of $k = 2$ letters, while ciphertext message units are blocks of $l = 3$ letters. The public key is $n = 1643$.

(i) Encrypt the plaintexts "Math" and "Info".

(ii) Decrypt the ciphertexts, knowing that $n = 31 \cdot 53$.

**3.** Use the 27-letter alphabet from the course (_ABC...XYZ with numerical equivalents 0,1,...,26) for ElGamal encryption and decryption. Plaintext message units are blocks of $k = 2$ letters, while ciphertext message units are blocks of $l = 3$ letters. The public key is $(p, g, g^a) = (2357, 2, 1185)$.

(i) Encrypt the plaintexts "Math" and "Info".

(ii) Decrypt the ciphertexts, knowing that $a = 1751$.

**4.** Example from Moodle.