IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises V.

1. Consider the RSA cryptosystem with $p = 43$, $q = 59$ and $d = 937$. Determine e and encrypt the plaintext 134879475204.

2. Let $n = pq$ where p and q are prime numbers. Show that $p + q = n - \varphi(n) + 1$.

3. Suppose a message w was encrypted by the RSA cryptosystem twice. Encryption with an exponent-modulus (e, n) pair $(17, 247021)$ produced the cryptotext $c_1 = 243247$. Another encryption of w with $(71, 247021)$ yielded $c_2 = 83123$. Determine w without factoring n.

4. Let p, q be primes such that $p \neq q$. Denote

$$n = pq, \quad \phi(n) = (p-1)(q-1), \quad g = \gcd(p-1, q-1).$$

   Prove that

$$a^{\phi(n)/g} \equiv 1 \pmod{n}$$

   for all a satisfying $\gcd(a, n) = 1$.

5. Suppose there is a polynomial time algorithm (with respect to the size of n) to find a nontrivial solution of the modular quadratic equation

$$a^2 \equiv 1 \pmod{n}.$$

   Show that you can find a factor of n in polynomial time (with respect to the size of n) using this algorithm.

6. Design of parameters for the RSA cryptosystem starts with choosing two large prime numbers. Because these prime numbers are part of the private key, they have to be chosen very carefully. More precisely, they need to be chosen at random by a cryptographically secure random number generator. Failing to do so can lead to problems. Consider the following set of RSA moduli, chosen by an *imperfect* random number generator, biased towards some numbers (some numbers appear with larger probability than others). Determine which of these moduli are secure. Do not use brute force factorization.

$$\{8844679, 11316499, 13490941, 18761893, 21799573,$$
$$22862761, 48456493, 43831027, 58354333, 60785419\}$$

7. Consider the McEliece cryptosystem with

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

   where G is the generator matrix of a $[9, 5, d]$ Goppa code with $d \geq 3$.

   (a) Compute G'.

   (b) Decode cryptotext $c = 001001110$.