ECRYPT- Problems for the midterm test #3, 20.01.2017

Problem # 1 Compute the following Legendre's symbols:

a) $\left(\frac{128}{5}\right)$, b) $\left(\frac{35}{7}\right)$, c) $\left(\frac{56}{13}\right)$

Problem # 2 Compute the following Jacobi's symbols:

a) $\left(\frac{56}{15}\right)$, b) $\left(\frac{13}{20}\right)$, c) $\left(\frac{57}{21}\right)$, d) $\left(\frac{13}{35}\right)$, e) $\left(\frac{12}{45}\right)$

Problem #3 Verify if the following congruencies have solutions

a) $x^2 \equiv 127 \pmod{13}$
b) $x^2 \equiv 8 \pmod{17}$

Problem #4 Give an example of a pseudoprime number

a) to the base 3

b) to the base 5

Problem # 5
Assume $k \in N$ and $GF(2^k)[x]$ is a ring of polynomials with coefficients in the field $GF(2^k)$. Prove, that if $r \in N$, $n \in N$, $n \geq 2$ and x^r is a polynomial from the ring of polynomials $GF(2^k)[x]$, then we have:

$$x^r \pmod{(x^n + 1)} = x^{r \pmod{n}}$$

Problem # 6
Propose a Shamir's algorithm of secret sharing for $n = 5$ users and the threshold $t = 3$. Compute shares of all users for a secret 8.

Problem # 7
Propose a Shamir's algorithm of secret sharing for $n = 6$ users and the threshold $t = 4$. Compute shares of all users for a secret 10.

Problem # 7

Design a public key cryptosystem RSA for “small numbers”. Cipher an exemplary plain text message and decipher obtained cryptogramme.

Problem # 8

Design a public key cryptosystem ElGamal for “small numbers”. Cipher an exemplary plain text message and decipher obtained cryptogramme.

Problem # 9

Design an ElGamal signature algorithm for “small numbers”. Sign an exemplary plain text message and verify correctness of the signature.