ECRYPT Problems preparing for the TEST #2

28.12.2016

Problem # 1

Describe the ElGamal signature algorithm and prove that verification formula is true when the signature parameters are correct.

Problem # 2

Describe the Nyberg-Rueppel signature algorithm and prove that verification formula is true when the signature parameters are correct.

Problem # 3

Solve the following set of congruencies :

$x \equiv 6 \pmod 7$
$x \equiv 4 \pmod 5$
$x \equiv 10 \pmod{11}$
$x \equiv 12 \pmod{13}$
$x \equiv 16 \pmod{17}$

Problem # 4

Assume we use RSA (with $n = p \cdot q$) and we have two cryptograms c_1 and c_2 of the same plain text message *m* which are ciphered with two different public keys e_1 and e_2 , where $GCD(e_1, e_2) = 1$. Prove that we can in easy way compute the plain text message (without private keys).

Problem # 5

Find the last 4 decimal digits of the number 2^{10^6} using Chinese Remainder Theorem.

Problem # 6

Assume we have two independent random variables X_1, X_2 with values in the set $Z_2 = \{0,1\}$.

Prove that if X_2 has a uniform distribution then $X_1 \oplus X_2$ has also the uniform distribution.

(This fact is known from the protocol “coin tossing by phone”)

Problem # 7

Assume we have two independent random variables X_1, X_2 with values in the set $Z_n = \{0,1,2,..n-1\}$. Prove that if X_2 has a uniform distribution then $X_1 \oplus_n X_2$ has also the uniform distribution.

Problem # 8

Compute the following values: a) $\varphi(\varphi(5358))$, b) $\varphi(\varphi(3458))$, c) $\varphi(\varphi(2^{1000}))$, where φ is the Euler's function.

Problem # 9

Assume $GF(2^k)[x]$ (where k is a fixed natural number) is a ring of polynomials with coefficients in the field $GF(2^k)$. Prove that for every polynomial x^n (where $n \in N$) from $GF(2^k)[x]$ we have

$$x^n (\mathrm{mod}(x^4 + 1)) = x^{n(\mathrm{mod}4)}$$

Problem # 10

How many times we have to repeat experiments in the cave of Zero Knowledge to obtain probability of fraud less then 10^{-10}.

Problem # 11

Describe the Fiat-Shamir entity authentication protocol. How many times we have to repeat the Fiat-Shamir protocol to obtain the probability of error less than 100^{-100}.

Problem # 12

Assume we test primality of odd natural numbers with the probabilistic Miller-Rabin test. Assess probability of the fact that an odd composite number *n* is accepted as a prime for a given security parameter $t \in N$.

Can the Miller-Rabin test qualify a prime as a composite number ?

How many experiments (random choices of the basis *a*) we have to do to be sure with probability $\geq 1 - 10^{-1000}$ that the tested number *n* is a prime.

Problem # 13

Assume we test primality of natural numbers with the probabilistic Solovay-Strassen test. Assess probability of the fact that an odd composite number *n* is accepted as a prime for a given security parameter $t \in N$.

Can the Solovay-Strassen test qualify a prime as a composite number ?

How many experiments (random choices of the basis *a*) we have to do to be sure with probability $\geq 1-10^{-1000}$ that the tested number *n* is a prime.

Problem # 14

Describe the field F_9 (i.e, the field $GF(3^2)$).

Problem # 15

What is it a pseudoprime number. Give an example of the pseudoprime number for the basis 2.

Problem # 16

Solve the following set of 4 congruencies

$x \equiv 3 \pmod 5$
$x \equiv 6 \pmod 7$
$x \equiv 7 \pmod{11}$
$x \equiv 7 \pmod{13}$

Problem # 17

Solve the following set of 3 congruencies :

$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv 3 \pmod{11}$

Problem # 18

Assume we have a well defined RSA cryptosystem with $n = p \cdot q$, a public key e and a private key d. Is it possible that for some plain text messages m we have $m^e \pmod m = m$?

It would mean that there are messages $m \in Z_n$ which are not encrypted correctly.

Problem # 19

Assume we have a hash function MD5. How many independent experiments (consisting in computation at random a hash value) we have to do to be sure that with probability $\geq 1/2$ there are 2 hash values which are identical (see birthday problem).

Problem # 20

We have two numbers $(1,2,3)$ and $(3,4,5)$ given in RNS notation with the moduli: $m_1 = 3$, $m_1 = 7$, $m_3 = 11$. Add and multiply these numbers using RNS algorithms. Verify if the results are correct.

Problem # 21

Define the Diffie-Hellman protocol of key exchanging. Why is it a secure protocol ?

Problem # 22

Compute values of the following Legendre's symbols

a) $\left(\frac{35}{7}\right)$

b) $\left(\frac{64}{5}\right)$

Solution

a) $\left(\frac{35}{7}\right) = \left(\frac{35(\mathrm{mod}\,7)}{7}\right) = \left(\frac{0}{7}\right) = 0$

b) $\left(\frac{64}{5}\right) = \left(\frac{64(\mathrm{mod}\,5)}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\cdot\left(\frac{2}{5}\right) = 1$

■

Problem # 23

Compute values of the following Legendre's symbols knowing that 1097 is a prime.

a) $\left(\frac{5}{1097}\right)$

b) $\left(\frac{7}{1097}\right)$

c) $\left(\frac{2}{1097}\right)$

Solution

From the law of quadratic reciprocity we have:

a) $\left(\frac{5}{1097}\right)\cdot\left(\frac{1097)}{5}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{1097-1}{2}}=1$

but $\left(\frac{1097}{5}\right)=\left(\frac{1097(\mathrm{mod}\,5)}{5}\right)=\left(\frac{2}{5}\right)=-1$ then also $\left(\frac{5}{1097}\right)=-1$

b) $\left(\frac{7}{1097}\right)\cdot\left(\frac{1097}{7}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{1097-1}{2}}=(-1)^{1644}=1$

but $\left(\frac{1097}{7}\right)=\left(\frac{1097(\mathrm{mod}\,7)}{7}\right)=\left(\frac{5}{7}\right)=-1$ then also $\left(\frac{7}{1097}\right)=-1$

c) From a general property of the Legendre symbol we have for every odd prime p

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

then $\left(\frac{2}{1097}\right)=(-1)^{(p^2-1)/8}$

■