ECRYP PROBLEMS FOR THE MIDTERM TEST #1

7.04.2018

Problem # 1

Alice and Bob use a binary Vernam's cryptosystem with a secret key $k = k_1 k_2 ... k_r$ where $k_i \in \{0,1\}$. Assume we know a plain text message $m = m_1 m_2 ... m_r$, where $m_i \in \{0,1\}$ and a corresponding cryptogram $c = c_1 c_2 ... c_r$ where $c_i \in \{0,1\}$. Compute the secret key $k = k_1 k_2 ... k_r$ from $m = m_1 m_2 ... m_r$ and $c = c_1 c_2 ... c_r$.

Problem # 2

Compute inverses of 7, 8, 9 a) in the multiplicative group Z^*_{11} b) in the multiplicative group $Z^*_{13.}$

Problem # 3

Compute inverses of 4,5,6, in the multiplicative groups Z^*_{13} and Z^*_{15}. List all elements in the multiplicative groups Z^*_{13} and Z^*_{15}.

Problem # 4

Compute all generators

1) of the multiplicative group Z^*_{17}
2) of the multiplicative group $Z^*_{13.}$

Problem # 5

Compute $\log_5 8$ in the multiplicative group Z^*_{13} and in the the multiplicative group Z^*_{19}.

Problem # 6

Give an example proving that the assumption in RSA definition: „*n* is a square-free number" is important.

Problem # 7

Assume we have a RSA cryptosystem with $n = p \cdot q$ (where *p* and *q* are secret different primes) and e is a public key. Prove that factorization of n breaks the RSA cryptosystem.

Problem #8

Assume we deal with the RSA cipher with $n = p \cdot q$ and RSA has two different public keys e_1 and e_2 which are relatively prime i.e. $GCD(e_1, e_2) = 1$. Prove that if we have two cryptogrammes c_1 and c_2 of the unknown plain text message $m \in Z_n$,

c_1 (cryptogramme obtained with e_1) and

c_2 (cryptogramme obtained with e_2)

then we can easily compute the plain text message $m \in Z_n$ from c_1 and c_2.

Problem # 9
Add the following polynomials (bytes) in the quotient ring
$Z_2[x]/(x^8+x^4+x^3+x+1)=GF(2^8)$:

a) ‘57’+’02’ b) ‘03’+’03’ c) ‘FF’+’0F’

Hint: see AES

Problem # 10
Multiply the following polynomials (bytes) in the quotient ring:
$Z_2[x]/(x^8+x^4+x^3+x+1)=GF(2^8)$

a) ‘57’*’02’ b) ‘57’*’04’ c) ‘57’*’10’

Hint: see AES

Problem # 11
Solve the following set of 4 congruencies :

x ≡ 3 (mod 7)
x ≡ 3 (mod 5)
x ≡ 3 (mod 11)
x ≡ 3 (mod 13)

Problem # 12
Solve the following set of 4 congruencies :

x ≡ 4 (mod 5)
x ≡ 6 (mod 7)
x ≡ 10 (mod 11)
x ≡ 12 (mod 13)

Problem # 13
Solve the following set of 5 congruencies :

x ≡ 5 (mod 7)
x ≡ 3 (mod 5)
x ≡ 9 (mod 11)
x ≡ 11 (mod 13)
x ≡ 15 (mod 17)

Problem # 14

Solve the following set of 3 congruencies

x ≡ 1 (mod 7)
x ≡ 2 (mod 5)
x ≡ 3 (mod 11)

Problem #15

Solve the following set of congruencies:

x ≡ 3 (mod 7),
x ≡ 9 (mod 13),
x ≡ 1 (mod 5) ,
x ≡ 7 (mod 11)

Problem # 16

Solve the following set of congruencies :

x ≡ 3 (mod 7)
x ≡ 3 (mod 5)
x ≡ 7 (mod 11)
x ≡ 7 (mod 13)

Problem # 17

Compute values of the Euler phi function

a) φ (3458), b) φ (3459), c) φ (5357) , d) φ (5358) , e) φ (2^{1000}), f) $\varphi(10^{1000})$

Problem # 18

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

Problem # 19

Assume $n, a \in N$ and $n \geq 2$. Prove that if $GCD(a,n) = 1$ then

$$a^{m \pmod{\varphi(n)}} \equiv a^m \pmod{n}$$

where φ is the Euler function.

Problem # 20

Prove that the polynomial $x^2 + 1$ is irreducible in the ring $Z_3[x]$ and describe the field $GF(9)$ (i.e. F_9).

Problem # 21

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 # 22

Design an ELGamal cryptosystem for the field F_{19}.

Problem # 22

Design a RSA cryptosystem for "small numbers".

Problem # 23

Compute three last decimal digits of the number 2^{1000} (in common decimal notation).

Problem # 24

Compute two last digits of the number 2^{1000} (in common radix 7 notation).

Problem # 25

Compute three last digits of the number 2^{10^6}

a)In common notation with radix $W = 10$ (common decimal notation)

b)In common notation with radix $W = 7$

Problem # 26

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

Problem # 27

Using the Extended Euclid's Algorithm compute inverses of the following polynomials in the quotient ring: $Z_2[x]/(x^8+x^4+x^3+x+1) = GF(2^8)$

a) '10' b) '04' c) '57'

Hint: see AES

Problem # 28

Describe a round in DES. What is it the S-box in DES? Explain the method applied for S-box description in DES.

Problem # 29

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

Problem # 30

Describe the ElGamal public key cipher and design an example of the cipher "for small numbers" with an example of ciphering.

Problem # 31

Design the ELGamal cryptosystem for the field F_{19}.

Problem #32

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 "fair coin tossing by phone")

The same in more strict formulation:

Prove the following theorem which is a crucial point for the Blum-Micali protocol (protocol of the fair coin tossing by phone). If $X_1 : \Omega \to \{0,1\}$ and $X_2 : \Omega \to \{0,1\}$ are two independent random variables defined on the probabilistic space $(\Omega, \mathcal{M}, P)$ and a random variable $X_2 : \Omega \to \{0,1\}$ has the uniform distribution on the set $\{0,1\}$ then the function defined by the formula $Y = X_1 \oplus X_2$ (addition modulo 2) is a random variable with the uniform probability distribution on the space $\{0,1\}$.

Solution

1.At first we prove that the function $Y = X_1 \oplus X_2$ is a random variable. In general if $(\Omega, \mathcal{M})$ is a measurable space and $(E_t, \mathcal{F}_t)_{t\in T}$ is an arbitrary family of measurable spaces and for every $t \in T$ the function $f_t : \Omega \to E_t$ $(\mathcal{M}, \mathcal{F}_t)$ is measurable then the function $\prod_{t\in T} f_t : \Omega \to \prod_{t\in T} E_t$ is $(\mathcal{M}, \prod_{t\in T} \mathcal{F}_t)$ measurable too. Applying this general fact to our situation we have that the function (X_1, X_2) is $(\mathcal{M}, 2^{\{0,1\}} \otimes 2^{\{0,1\}})$ measurable. The function $S : \{0,1\} \times \{0,1\} \ni (x_1, x_2) \to x_1 \oplus x_2 \in \{0,1\}$ is of course $(2^{\{0,1\}} \otimes 2^{\{0,1\}}, 2^{\{0,1\}})$ measurable then $Y = X_1 \oplus X_2$ as a superposition of two measurable functions (X_1, X_2) and S is $(\mathcal{M}, 2^{\{0,1\}})$ measurable then it is a random variable.

2. Now we prove that the probability distribution of the random variable $Y = X_1 \oplus X_2$ is uniform. Denote

$$A_1 = \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 0\}, \qquad B_1 = \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 1\}$$
$$A_0 = \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 0\}, \qquad B_0 = \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 1\}$$

Sets A_0, A_1, B_0, B_1 are disjoint in pairs. Denote additionally $P(X_1 = 0) = p_0$, $P(X_1 = 1) = p_1$.
Random variables X_1 and X_2 are independent then we have

$$P(Y=1) = P(A_1 \cup B_1) = P(A_1) + P(B_1) = P(X_1 = 1) \cdot P(X_2 = 0) + P(X_1 = 0) \cdot P(X_2 = 1) = p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2}$$

(because $p_0 + p_1 = 1$) and similarly

$$P(Y=0) = P(A_0 \cup B_0) = P(A_0) + P(B_0) = P(X_1 = 0) \cdot P(X_2 = 0) + P(X_1 = 1) \cdot P(X_2 = 1) = p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2}$$

then the random variable $Y = X_1 \oplus X_2$ has the uniform probability distribution. ■

Problem # 33
Describe the ElGamal signature algorithm and prove that verification formula is true when the parameters are correct.

Problems # 34

We have two numbers $a = (3,4,5)$ and $b = (2, 1, 8)$ written in RNS notation for moduli $m_1 = 5$, $m_2 = 7$, $m_3 = 11$. Add and multiply these numbers.