Modern Cryptography **Autumn 2018**

Assignment 3

1. Using the extended Euclidean algorithm, find the multiplicative inverse of 1234 mod 4321

2. For polynomial arithmetic with coefficients in Z_{10}, perform the following calculations $(7x+2)-(x^2+5)$

3. Determine which of the following are reducible over GF(2).
   a. $x^3 + 1$
   b. $x^3 + x^2 + 1$
   c. $x^4 + 1$(be careful)

4. Determine the gcd of the following pairs of polynomials.
   a. $x^3 + x + 1$ and $x^2 + x + 1$ over GF(2)
   b. $x^3 - x + 1$ and $x^2 + 1$ over GF(3)

5. Compute $[101^{4,800,000,002}\ mod\ 35]$ (by hand).

6. compute $46^{51}\ mod\ 55$ (by hand) using the Chinese remainder theorem.

7. Formally define the CDH assumption. Prove that hardness of the CDH problem relative to $\mathcal{G}$ implies hardness of the discrete-logarithm problem relative to $\mathcal{G}$, and that hardness of the DDH problem relative to $\mathcal{G}$ implies hardness of the CDH problem relative to $\mathcal{G}$.

8. Describe a man-in-the-middle attack on the Diffie-Hellman protocol where the adversary shares a key k_A with Alice and a (different) key k_B with Bob, and Alice and Bob cannot detect that anything is wrong.

9. Show that any two-round key-exchange protocol (that is, where each party sends a single message) satisfying Definition 10.1 can be converted into a CPA-secure public-key encryption scheme.

10. Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let G be the group of squares modulo p (so G is a subgroup of Z_p^* of order q), and let $\mathfrak{g}$ be a generator of G. The private key is (G,$\mathfrak{g}$,q,x) and the public key is (G,$\mathfrak{g}$,q,h), where $h = \mathfrak{g}^x$ and $x \in Z_q$ is chosen

uniformly. To encrypt a message $m \in Z_q$, choose a uniform $r \in Z_q$, compute $c_1 := g^r \, mod \, p$ and $c_2 := h^r + m \, mod \, p$, and let the ciphertext be $\langle c_1, c_2 \rangle$. Is this scheme CPA-secure? Prove your answer.

Note:

Definition 10.1: A key-exchange protocol $\prod$ is secure in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function negl such that

$$Pr[KE^{eav}_{\mathcal{A},\prod}(n) = 1] \leqslant \frac{1}{2} + negl(n).$$

(1) Due date: Sunday, November 18, 2018, at 23:59. Send your assignment to the following email: 2821785913@qq.com

(2) Assignment should be named by UNo+Name+A3.docx/doc/pdf.

(3) Penalty for late submission: 15% of the total marks for every day after the deadline.

(4) Answer ALL 10 questions.