# CS304: Introduction to Cryptography & Network Security

**Endsem** — **Marks: 25**

Course Instructor: Dr. Dibyendu Roy — Time Limit: 100 min

Instructions: Clearly write your name and roll number. Solutions must be written clearly.

---

**(Q1)** **[4 marks]**

Write down signature generation and verification algorithm for Elliptic curve based digital signature scheme.

**(Q2)** **[4 marks]**

Suppose that Bob adopts the RSA cryptosystem with primes $p = 59$ and $q = 71$. He chooses the (public key) encryption exponent to be $e = 1077$. Write each answer as an integer in $\{1, 2, \ldots, m-1\}$ if you are working modulo $m$.

(a) Show that Bob's choice of encryption exponent is legitimate, and find his corresponding (private key) decryption exponent $d$.

(b) Suppose that Alice encrypts the plaintext message $P = 1234$ using the RSA cryptosystem with Bob's public key $(n, e) = (4189, 1077)$. What is the resulting ciphertext that would be sent to Bob?

(c) Go through the decryption process that would need to be done at Bob's end using his private key $(n, d)$ with decryption exponent that was determined in item (a).

**(Q3)** **[4 marks]**

Let $p$ be a large prime number and $g$ be the generator of the group $(\mathbb{Z}_p^*, \times \mod p)$. Here $g$ and $(\mathbb{Z}_p^*, \times \mod p)$ are public. Let the private and public keys of Alice be $x, y$ respectively (so we have $y \equiv g^x \mod p$). In order to sign a message $m \in \mathbb{Z}_{p-1}$, Alice chooses $k$ randomly from $\mathbb{Z}_{p-1}$ and computes $r \equiv g^k \mod p$ and $s = (xr + km) \mod (p-1)$. Alice's signature on $m$ is the pair $(r, s)$. Show how the signature $(r, s)$ on $m$ can be verified.

**(Q4)** **[4 marks]**

Using Chinese Remainder Theorem find $x$ such that

$$
\begin{aligned}
x &\equiv 2 \mod 23,\\
x &\equiv 3 \mod 41,\\
x &\equiv 2 \mod 61.
\end{aligned}
$$

2×30
2×10×3

RSA

**(Q5)** **[4 marks]**

Let $H : X \to Y$ be a secure hash function with the property $|X| > |Y|$. Prove that the collision finding algorithm will have $O(\sqrt{|Y|})$ complexity.

**(Q6)** **[5 marks]**

Suppose that $n = pq$ is an RSA modulus (i.e., p and q are distinct odd primes), and let $\alpha \in \mathbb{Z}_n^*$. Suppose that $\gcd(p-1, q-1) = 2$, and we have an algorithm $\mathcal{A}$ that solves the Discrete Logarithm problem in the subgroup $< \alpha >$ where $\alpha \in \mathbb{Z}_n^*$ has order $\frac{\phi(n)}{2}$ (here $< \alpha > = \{1, \alpha, \alpha^2, \ldots, \alpha^{\frac{\phi(n)}{2}-1}\}$). That is, given any $\beta \in < \alpha >$, the algorihtm $\mathcal{A}$ will find the discrete logarithm $a = \log_\alpha \beta$, where $0 \le a \le \frac{\phi(n)}{2} - 1$. (The value $\frac{\phi(n)}{2}$ is secret however.) Suppose we compute $\beta = \alpha^n \mod n$ and then we use $\mathcal{A}$ to find $a = \log_\alpha \beta$. Assuming that $p > 3$ and $q > 3$, prove that $n - a = \phi(n)$. Also describe how $n$ can easily be factored, given the discrete logarithm $a = \log_\alpha \beta$ from the algorithm $\mathcal{A}$.

22+1