Homework 7
COMP543 Fall 2020 - Modern Cryptography

Erhan Tezcan 0070881

20.11.2020

---

1. Quesitons

Q1: Compute the final two (decimal) digits of 3^{1000} (by hand). Hint: The answer is $[3^{1000} \bmod 100]$.

A1: Remember a theorem[1] and corollary[2]:

Theorem 1.1. *Let $N = \Pi_i p_i^{e_i}$ where $\{p_i\}$ are distinct primes and $e_i \geq 1$. Then we can find the order:*

$$|\mathbb{Z}_N^*| = \phi(N) = \Pi_i p_i^{e_i - 1}(p_i - 1)$$

Corollary 1.2. *For a finite group G with order $m > 1$, $\forall x \in G$ and integers x it holds that:*

$$g^x = g^{[x \bmod m]}$$

We have $100 = 2^2 5^2$ so we can find the order $\mathbb{Z}_1 00^* = 2^{2-1}(2-1)5^{2-1}(5-1) = 40$. So, $3^{1000} = 3^{[1000 \bmod 40]} \bmod 100$. We find the result 1 from this.

Q2: Compute $[4651 \bmod 55]$ (by hand) using the Chinese Remainder Theorem.

A2: We shall notice that $55 = 11 \times 5$ and $gcd(11, 5) = 1$. CRT says that $\mathbb{Z}_{55} \simeq \mathbb{Z}_{11} \times \mathbb{Z}_5$. An instance of this isomorphism is:

$$4651 \bmod 55 \iff (9 \bmod 11)(1 \bmod 5)$$

Then we apply the algorithm in page 301 (right above example 8.30) in KL Book 2nd ed.:

(1) $x \times 5 + y \times 11 \implies x = -2, y = 1$
(2) $1_p = 11 \bmod 55, 1_q = -10 \bmod 55 = 45 \bmod 55$
(3) $x = (1 \times 11 + 9 \times 45) \bmod 55 = 31 \bmod 55$

The result is therefore 31.

Q3: What is a group? What are the properties of a group? Which groups are called abelian? Explain your answer.

---

[1] Theorem 8.19 from KL Book 2nd ed.

[2] Corollary 8.15 from KL Book 2nd ed.

A3: A group is a way to reason about objects with same underlying nature and share the same mathematical structure. More formally, a group $(G, \cdot)$is a set G along with a binary operation $\cdot$ for which the following hold:

- **(Closure)**: $\forall g, h \in G : g \cdot h \in G$
- **(Existence of Identity)**: $\exists e \in G : \forall g \in G$ s.t. $e \cdot g = g \cdot e = g$
- **(Existence of Inverses)**: $\forall g \in G : \exists h \in G$ s.t. $h \cdot g = g \cdot h = e$. We also denote and inverse of g as $h = g^{-1}$
- **(Associativity)**: $\forall g_1, g_2, g_3 \in G : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

A group $(G, \cdot)$ is Abelian if the binary operation $\cdot$ is **commutative**: $\forall g, h \in G : g \cdot h = h \cdot g$.

Q4: For each of the following groups, write down their elements and inverses[3] of each elements.

a. $\mathbb{Z}_6$
b. $\mathbb{Z}_6^*$
c. $\mathbb{Z}_7$
d. $\mathbb{Z}_7^*$

A4:

a. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 have an inverse, explained in next bullet.
b. $\mathbb{Z}_6^* = \{1, 5\}$ and their inverses are respectively: $\{1, 5\}$.
c. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, all except 0 have an inverse, explained in the next bullet.
d. $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ and their inverses are respectively: $\{1, 4, 5, 2, 3, 6\}$.

Q5: What is a cyclic group? Is the multiplicative group $\mathbb{Z}_7^*$ a cyclic group? If yes, what is the generator? What is the order of element 2 in this group? Explain your answer.

A5: A group G where $|G| = n$ is cyclic if $\exists g \in G$ s.t. $\{1, g^1, g^2, \ldots, g^{n-2}\} = G$, and such g is called a "generator". The group $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ is a cyclic group, which we know from Euler's theorem that says for a prime p the group $\mathbb{Z}_p^*$ is cyclic. The generator of this group is 3: $\{1, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^*$. The order of 2, also shown as $ord_7(2)$ is 3, because $\{1, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$ and the size of this group is 3.

Q6: Formally define the RSA assumption.

[3]The inverse of x in $\mathbb{Z}_N$ is an element y in $\mathbb{Z}_N$ such that $xy = 1$ in $\mathbb{Z}_N$.

A6: The RSA assumption is that there exists a `GenRSA` algorithm relative to which the RSA problem is **hard**. `GenRSA` is a probabilistic polynomial-time algorithm that when given 1^n, it outputs a modulus N that is the product of two n-bit long primes e and d such that $gcd(e, \phi(N)) = 1$ and $ed = 1 \bmod \phi(N)$.

Q7: Formally define the Discrete Logarithm assumption.

A7: The Discrete Logarithm assumption is the assumption that solving the discrete logarithm $log_g h$ for a cyclic group G, generator g and $h \in G$, is **hard**.