EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Endsem Exam: 40 points Date: November 21, 2024

1. [5 points] Solve the following system of congruences using the Chinese remainder theorem. Show your steps and reduce your answer to an element in $\mathbb{Z}_{746130}$.

$$\begin{aligned} x &= 2 \bmod 11, \\ x &= 3 \bmod 14, \\ x &= 4 \bmod 15, \\ x &= 5 \bmod 17, \\ x &= 6 \bmod 19. \end{aligned}$$

2. Alice is using the plain RSA signature scheme with public key $\langle 143, 7 \rangle$.
   (a) [2 points] What is Alice's private key?
   (b) [3 points] What is the plain RSA signature corresponding to the message $m = 2$? Reduce your answer to an integer in the set $\{0, 1, \ldots, 142\}$.

   Hint: Let p_1, p_2 be relatively prime positive integers. Then the unique solution modulo $M = p_1 p_2$ of the system of congruences

$$\begin{aligned} x &= a_1 \bmod p_1 \\ x &= a_2 \bmod p_2 \end{aligned}$$

   is given by $x = a_1 M_1 y_1 + a_2 M_2 y_2 \bmod M$ where $M_i = \frac{M}{p_i}$ and $M_i y_i = 1 \bmod p_i$ for $i = 1, 2$.

3. [5 points] Find the four square roots of 267 in $\mathbb{Z}_{1333}^*$. Show your steps and express the square roots as integers in the range $\{1, 2, \ldots, 1332\}$.

   Hint: Note that $1333 = 31 \times 43$. Suppose $N = pq$ where $\gcd(p, q) = 1$ and $p, q > 1$. Let X, Y be integers such that $Xp + Yq = 1$. Consider the mapping $f : \mathbb{Z}_N \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$ given by $f(x) = (x \bmod p, x \bmod q)$. Then the preimage of $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ under f is given by $x = aYq + bXp \bmod N$.

4. [5 points] For prime $p > 2$ and $x \in \mathbb{Z}_p^*$, the Jacobi symbol of x modulo p is given by

$$\mathcal{J}_p(x) = \begin{cases} +1 & \text{if } x \in \mathcal{QR}_p, \\ -1 & \text{if } x \in \mathcal{QNR}_p. \end{cases}$$

   In the above definition, the sets $\mathcal{QR}_p$ and $\mathcal{QNR}_p$ correspond to quadratic residues and quadratic non-residues modulo p, respectively. Prove the following.
   (a) The only square roots of 1 in $\mathbb{Z}_p$ are $+1$ and -1.
   (b) $\mathcal{J}_p(x) = x^{\frac{p-1}{2}} \bmod p$

   Hint: You can assume that $\mathbb{Z}_p^*$ is cyclic without proof.

5. In the coin-flipping over telephone protocol, Alice sends the integer $N = 84281$ to Bob. Bob picks $x = 300$ and sends $a = x^2 \bmod N = 5719$ to Alice.
   (a) [3 points] After receiving a from Bob, suppose Alice sends $z = 4365$. Who wins in the protocol? Explain your answer.
   (b) [2 points] What are the other three values which Alice can send as z in the protocol? Specify numerical values in $\mathbb{Z}_N$.

6. Let $N = pq$ where p and q are distinct odd primes. Suppose the public key in the Goldwasser-Micali encryption scheme is $\langle N, z\rangle$ where z is a quadratic non-residue modulo N with Jacobi symbol $+1$, i.e. $z \in \mathcal{QNR}_N^{+1}$. The private key is the factorization of N.

   (a) [2 points] Describe the encryption and decryption procedures of the Goldwasser-Micali encryption scheme for a message space $\mathcal{M} = \{0,1\}^n$ where $n \geq 1$.

   (b) [3 points] Prove that the Goldwasser-Micali encryption scheme is **not** CCA-secure.

   Note 1: The *CCA indistinguishability experiment* $\mathtt{PubK}^{\mathtt{cca}}_{\mathcal{A},\Pi}(n)$ where $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is described below.

   1. A key pair (pk, sk) is generated by running $\mathtt{Gen}(1^n)$.
   2. The adversary $\mathcal{A}$ is given pk and access to a decryption oracle $\mathtt{Dec}_k(\cdot)$. It outputs a pair of messages $m_0, m_1 \in \mathcal{M}_{pk}$ of the same length.
   3. A uniform bit $b \in \{0,1\}$ is chosen. Ciphertext $c \leftarrow \mathtt{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. c is called the *challenge ciphertext*.
   4. The adversary $\mathcal{A}$ continues to have oracle access to $\mathtt{Dec}_k(\cdot)$, but is not allowed to query the oracle on the challenge ciphertext itself. Eventually, $\mathcal{A}$ outputs a bit b'.
   5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If output is 1, we say that $\mathcal{A}$ succeeds.

   Note 2: A public-key encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ has **indistinguishable encryptions under a chosen-ciphertext attack**, or is **CCA-secure**, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that, for all n,

$$\Pr\left[\mathtt{PubK}^{\mathtt{cca}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathtt{negl}(n).$$

7. Bob is applying to become a pilot. He has to prove that he is not color-blind, i.e. he has to prove that he can distinguish between colors. For simplicity, let us assume that he only needs to prove that he can distinguish between the colors RED and BLUE. Alice has two pens which have the same shape and differ only in their color. One is RED in color and the other is BLUE in color.

   (a) [3 points] Design an interactive protocol which can be used by Bob to prove to Alice that he is not color-blind.

   (b) [2 points] Analyze your protocol and show that it satisfies the definition of an interactive proof system for the statement that Bob can distinguish between RED and BLUE.

   Note: Let $c, s : \mathbb{N} \to \mathbb{R}$ be functions satisfying $c(n) > s(n) + \frac{1}{p(n)}$ for some polynomial $p(\cdot)$.

   A pair of interactive machines (P, V) is called an **interactive proof system for a language** L if V is PPT and the following conditions hold:

   - **Completeness**: For every $x \in L$, we have $\Pr[\langle P, V\rangle(x) = 1] \geq c(|x|)$
   - **Soundness**: For every $x \notin L$ and every interactive machine B, we have $\Pr[\langle B, V\rangle(x) = 1] \leq s(|x|)$

8. [5 points] Prove that the El Gamal encryption scheme is CPA-secure if the decisional Diffie-Hellman (DDH) problem is hard relative to a cyclic group generation algorithm $\mathcal{G}$.

Note 1: Let $\mathcal{G}$ be a cyclic group generation algorithm that on input 1^n outputs a triple (G, q, g) where G is a cyclic group of prime order q having generator g.

We say the **DDH problem is hard relative to** $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function negl such that

$$\left| \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^{xy}) = 1] \right| \leq \mathsf{negl}(n)$$

where $x, y, z \in \mathbb{Z}_q$ are uniformly chosen

Note 2: The El Gamal encryption scheme is a triple of PPT algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ along with a cyclic group generation algorithm $\mathcal{G}$.

- Gen: Run $\mathcal{G}(1^n)$ to get (G, q, g) where G is a cyclic group of prime order q having generator g. Choose a uniform $x \in \mathbb{Z}_q$ and compute $h := g^x$. The public key is $\langle G, q, g, h \rangle$ and the private key is $\langle G, q, g, x \rangle$. The message space is G.
- Enc: For public key $pk = \langle G, q, g, h \rangle$ and message $m \in G$, choose a uniform $y \in \mathbb{Z}_q$. Output the ciphertext as $\langle g^y, h^y \cdot m \rangle$
- Dec: For private key $pk = \langle G, q, g, x \rangle$ and ciphertext $\langle c_1, c_2 \rangle$, output $\hat{m} = c_2 \cdot c_1^{-x}$.

Note 3: The **eavesdropping indistinguishability experiment** $\mathtt{PubK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$ where $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is described below.

1. A key pair (pk, sk) is generated by running $\mathtt{Gen}(1^n)$.
2. The adversary $\mathcal{A}$ is given pk. It outputs a pair of messages $m_0, m_1 \in \mathcal{M}_{pk}$ of the same length.
3. A uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \mathtt{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. c is called the *challenge ciphertext*.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If output is 1, we say that $\mathcal{A}$ succeeds.

Note 4: A public-key encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ has **indistinguishable encryptions in the presence of an eavesdropper**, or is **EAV-secure**, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that, for all n,

$$\Pr\left[\mathtt{PubK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathtt{negl}(n).$$

Note 5: A public-key encryption scheme which is EAV-secure is also CPA-secure since the adversary already has access to an encryption oracle (through the public key).