RSA and PKC

Anderson C A Nascimento, Ph.D.
Cryptology

November 21, 2016

Question 1. Let $\mathcal{G}$ be an abelian group. Prove that there is a unique identity in $\mathcal{G}$ and that every element in $\mathcal{G}$ has a unique inverse.

Question 2. Let $\mathcal{G}$ be a finite group, and $g \in \mathcal{G}$. Show that $< g >= g^0, g^1, g^2, \ldots$ is a subgroup of $\mathcal{G}$.

Question 3. Let p be a prime and $e \geq 1$ an integer. Show that

$$\phi(p^e) = p^e(p - 1.)$$

Let p, q be relatively prime. Show that $\phi(pq) = \phi(p).\phi(q)$. Finally, prove that for an integer $N = \prod_i p_i^{e_i}$, where p_i are distinct primes and $e_i \geq 1$, we have that $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$

Question 4. Prove that if $\mathcal{G}$ and $\mathcal{H}$ are groups then $\mathcal{G} \times \mathcal{H}$ is also a group ($\times$ is the cross product).

Question 5. Give a full proof of the chinese remainder theorem.

Question 6. We have seen in class that if $N = pq$ and $ed = 1 \mod \phi(N)$ then for all $x \in \mathcal{Z}_N^*$ we have that $(x^e)^d = x \mod N$. Show that this holds for all $x \in \mathcal{Z}_N$. (Use the chinese remainder theorem). What are the consequences of this result to the RSA encryption scheme?

Question 7. Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known then it is possible to compute p and q in polynomial time.

Question 8. Define CPA and CCA secure public key encryption schemes

Question 9. Describe the DDH assumption. Show that the ElGamal public key scheme is CPA secure if the DDH assumption holds

Question 10. A clever Brazilian graduate student decided to implement the RSA cryptosystem. In order to speed up the key generation process the student chosen the RSA modulus $N = p$, where p is a prime number. show that the resulting scheme is insecure.

Question 11. Describe the Extended Euclidean Algorithm and explain where it is used in the RSA and ElGamal crypto systems

Question 12. A clever Brazilian student came up with an interesting way of encrypting long messages with the RSA cryptosystem. Each letter of the alphabet is represented by an integer between 0 and 25. Each letter of a message is then encrypted by using the RSA scheme with a modulus n of 2048 bits. All the encrypted letters are sent to the receiver. Is this scheme secure? Explain.

Question 13. Does storing Hash(username || password) (hash of the username concatenated with the user's password) on the server better defend against an attacker who breaks into the server and tries to crack passwords than just storing Hash(password)?

Question 14. Consider the following protocol for two parties A and B to flip a fair coin (more complicated versions of this might be used for Internet gambling): (1) a trusted party T publishes her public key pk; (2) A chooses a random bit b_A, encrypts it using pk, and announces the ciphertext c_A to B and T ; (3) next, B acts symmetrically and announces a ciphertext $c_B \neq c_A$; (4) T decrypts both c_A and c_B, and the parties XOR the results to obtain the value of the coin. (a) Argue that even if A is dishonest (but B is honest), the final value of the coin is uniformly distributed. (b) Assume the parties use El Gamal encryption (where the bit b is encoded as the group element g^b). Show how a dishonest B can bias the coin to any value he likes. (c) Suggest what type of encryption scheme would be appropriate to use here. Can you define an appropriate notion of security and prove that your suggestion achieves this definition?

Question 15. Show that El Gamal is not CCA secure. Show that textbook RSA is not even CPA secure.

Question 16. The Tacoma Institute of Cryptology proposes the following scheme to make RSA secure against the chosen-plaintext attack. Let (e, n) be the RSA public key. To encrypt message m, generate a random number r, xor it with the message, and encrypt r using plain RSA. The ciphertext is the pair $(m \oplus r, r^e \mod n)$. Is this encryption scheme secure against the chosen-plaintext attack? Explain your answer.

Question 17. Give a precise security definition of a digital signature scheme. Is the textbook implementation of RSA secure according to your definition? Why? What can be done to fix RSA signatures?

Question 18. Show that if the RSA signature scheme is implemented without hash functions the resulting signature scheme is not secure.