

Name: Breno

pp. 1

1. (20pts) Let  $n, e$  be the public key and  $d$  the private key of an RSA cryptosystem. Describe:

- How to compute the encryption of a value  $m$ .

ciphertext  $c = m^e \pmod n$ .

- How to decrypt a ciphertext  $c$ .

plaintext  $m = c^d \pmod n$ .

2. (28pts) Solve the following numerical examples related to the RSA cryptosystem.

- Let  $p = 23$ ,  $q = 19$ . Compute  $n$  and  $\phi(n)$ .

$n = p \cdot q = 437$ .  $\phi(n) = \phi(437) = (p - 1)(q - 1) = 22 \cdot 18 = 396$ .

- Let  $p = 11$ ,  $q = 23$ ,  $n = 253$ , and  $\phi(n) = 220$ . Let  $e = 17$ . Which of the following is  $d$ ?:  
 $\{1, 4, 13, 219\}$ .

Answer: 13; Note that  $13 \cdot 17 = 221 \simeq 1 \pmod{220 = \phi(n)}$

- Let  $p = 7$ ,  $q = 11$ ,  $n = 77$ , and  $\phi(n) = 60$ , and let  $e = d = 11$ . Given  $M = 2$ , compute the encryption of  $M$ .

$C = M^e \pmod n : 2^{11} \pmod{77} = 2048 \pmod{77} = 46$ .

- With the same values as above, decrypt the ciphertext  $C = 75$ .

Note that  $75 = -2 \pmod{77}$ . Then  $M = C^d \pmod n : (-2)^{11} \pmod{77} = -46 \pmod{77} = 31$ .

3. (12pts) Answer TRUE or FALSE to each of the questions below?

- There is ONLY ONE value  $x$  in the set  $\{0, 1, \dots, 32299\}$  such that  $x = 243 \pmod{323}$  and  $x = 97 \pmod{100}$ . TRUE \*\*\*\*\*

- There is NO value  $x$  in the set  $\{0, 1, \dots, 47\}$  such that  $x = 4 \pmod{6}$  and  $x = 3 \pmod{8}$ .  
TRUE \*\*\*\*\*

- There are TWO values  $x$  in the set  $\{0, 1, \dots, 23\}$  such that  $x = 0 \pmod{4}$  and  $x = 2 \pmod{6}$ . TRUE \*\*\*\*\*

4. (28pts) In each of the cases below, decide if the Miller's algorithm indicates whether the number is COMPOSITE or POSSIBLY PRIME.
- $3^{1060} = 1 \pmod{1061}$ , therefore 1061 is POSSIBLY PRIME\*\*\*\*\*.
  - $1951 - 1 = 2 \cdot 975$ , and  $3^{975} = -1 \pmod{1951}$ . Therefore, 1951 is POSSIBLY PRIME\*\*\*\*\*.
  - $1813 = 4 \cdot 453$ , and  $2^{906} = 841 \pmod{1813}$ . Therefore, 1813 is COMPOSITE\*\*\*\*\*.
5. (15pts) Explain what a nonce is, and why are they useful in authentication protocols.

NONCE is a *value used only once*. It is a random or pseudo-random value added to messages in an authentication protocol to ensure liveness of communication. Reply messages include nonces that were sent in encrypted form in request messages to indicate that the reply is recent, avoiding replay attacks.

6. (32 pts) Suppose  $A$  and  $B$  know each other's public keys,  $PK_A$  and  $PK_B$ .  $A$  wants to communicate with  $B$ , and wishes to provide  $B$  with a proof that her communication request is current (not a replay). Also  $A$  requires that  $B$  similarly prove his identity and that it has received  $A$ 's request.  $A$  and  $B$  use a 3-pass protocol and nonces  $N_1, N_2$  to achieve this. In the first case, they use encryption, in the second case, they use signatures. Given the first message of each transaction, write the next two.

•

$$A \rightarrow B : ENC_{PK_B}(ID_A || N_1)$$

$$B \rightarrow A : ENC_{PK_A}(N_1 || N_2)$$

$$A \rightarrow B : ENC_{PK_B}(N_2)$$

•

$$A \rightarrow B : SIG_{PK_A}(ID_A || N_1)$$

$$B \rightarrow A : SIG_{PK_B}(N_1 || N_2)$$

$$A \rightarrow B : SIG_{PK_A}(N_2)$$

---

7. (15 pts) Explain what is a certificate, and why it is useful.

A (public key) certificate is a digitally signed statement to bind together a public key with identifiable information such as the name of a person or an organisation, their address, etc. The signer of the certificate should be trusted (known entity) or trustworthy (e.g., a trusted authority) in order to convey authenticity that a public key belongs to an individual.

8. (20pts) Describe in words the Miller-Rabin's algorithm for testing if a number is a composite or a possible prime. (Alternatively: Describe the Extended GCD algorithm.)

Only description of Miller-Rabin's provided. If  $n$  is the number being tested, first find the maximum 2-power  $2^k$  that divides  $n-1$ , i.e.,  $n-1 = 2^k q$ , where  $q$  is an odd integer. The algorithm then chooses a value  $a$  at random in  $\{1, \dots, n-1\}$ . Compute  $a^q, a^{2q}, a^{2^2q}, \dots, a^{2^{k-1}q}, a^{2^kq}$  (all mod  $n$ ). Then:

- if  $a^q \simeq 1 \pmod n$ , return "INCONCLUSIVE (POSSIBLY PRIME)."
- if  $a^{2^kq} \not\simeq 1 \pmod n$ , return "COMPOSITE."
- For the third case,  $a^q \not\simeq 1 \pmod n$  and  $a^{2^kq} \simeq 1 \pmod n$ . Let  $\ell \geq 1$  be the smallest value such that  $a^{2^\ell q} \simeq 1 \pmod n$ . Then if  $a^{2^{\ell-1}q} \not\simeq -1 \pmod n$  return "COMPOSITE." Otherwise, return "INCONCLUSIVE (POSSIBLY PRIME)."

It can be shown that, if  $n$  is composite, each randomly generated  $a$  has only 1/4 probability of returning "INCONCLUSIVE" as the result of the above experiment. Repeating the test multiple times can increase the confidence of a primality answer to a high level.