Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[5 parts, 1 point each]** Alice and Bob use RSA to communicate.

   (a) To make his RSA key pair, Bob selects $p = 71$ and $q = 101$. What are N and N'?

   $N = pq = \boxed{7171}$

   $N' = (p-1)(q-1) = \boxed{7000}$

   (b) Next, Bob needs to select an encryption exponent; to make encryption fast but nontrivial, he wants his encryption exponent e to be in the range $5 \le e \le 10$. Which exponent should Bob choose?

   Need e and $N' = 7000 = 7 \cdot (2 \cdot 5)^3 = 2^3 \cdot 5^3 \cdot 7$ to be relatively prime. So, pick $\boxed{e = 9}$.

   (c) Find the decryption exponent d.

   $7000 = 777 \cdot 9 + 7$

   $9 = 1 \cdot 7 + 2$

   $7 = 3 \cdot 2 + 1$

   $1 = 7 - 3 \cdot 2$

   $= 7 - 3(9 - 1 \cdot 7)$

   $= 4 \cdot 7 - 3 \cdot 9$

   $= 4(7000 - 777 \cdot 9) - 3 \cdot 9$

   $1 = 4 \cdot 7000 - 3111 \cdot 9$

   So $d \equiv -3111 \equiv \boxed{3889} \pmod{N'}$

   (d) What should Bob publish as his public key?

   $(N, e) = \boxed{(7171, 9)}$

   (e) Alice wants to send Bob $m = 1544$. What ciphertext should she send to Bob?

   Modulo N:

   $C \equiv m^e \pmod{N} \equiv (1544)^9 \equiv 3716 \cdot 1544$

   $\equiv \boxed{704} \pmod{7171}$.

   $(1544)^2 \equiv 3164$

   $(1544)^4 \equiv 180$

   $(1544)^8 \equiv 3716$

2. **[3 points]** Given that $N = 1994969$ and $N' = 1992144$, factor N.

$p+q = N - N' + 1 = 2826$

$x^2 - (p+q)x + N = x^2 - 2826x + 1994969$

$x = \dfrac{2826 \pm \sqrt{(2826)^2 - 4 \cdot 1994969}}{2}$

$= \dfrac{2826 \pm \sqrt{7986276 - 4 \cdot 1994969}}{2}$

$= \dfrac{2826 \pm \sqrt{6400}}{2} = \dfrac{2826 \pm 80}{2} = 1413 \pm 40$

$x = 1373, 1453$

So $\boxed{N = 1373 \cdot 1453}$.

3. **[2 points]** Alice publishes (N, e) as her public RSA key. Unfortunately, Alice did not pay attention in cryptography class and is willing to prove her identity by decrypting ciphertexts of random messages encrypted with her public key. Previously Eve intercepted a ciphertext c that Bob sent to Alice. What should Eve send to Alice under the guise of verifying Alice's identity that will allow her to decrypt c? Note: if Eve simply sends c to Alice, then Alice will recognize the decrypted plaintext and refuse Eve's request.

Eve should pick an integer k in $\mathbb{Z}_N^*$ at random and send Alice

$c' \equiv \boxed{k^e c \pmod N}$.

Alice Responds with $(c')^d \equiv (k^e c)^d \equiv k^{ed} c^d \equiv km$.

Eve then computes $k^{-1}(km) \equiv m \pmod N$.