Homework # 5 Due 11pm on Wed March 14

CS 178 Intro to Crypto

1. Use the Fermat's test to prove that 1111 is not a prime number.
2. Use the Fermat's test to prove that $F_5 = 2^{2^5} + 1 = 4294967297$ is not a prime number.
3. Use the Miller-Rabin test to prove that $F_5 = 2^{2^5} + 1 = 4294967297$ is not a prime number.
4. Determine all possible encryption exponents for the RSA modulus $n = 437$.
5. Alice encrypts a message m with Bob's public key RSA key $(899, 11)$. The ciphertext is 468. Determine the plaintext?
6. How many multiplications and squarings are required for an RSA encryption with the encryption exponent $e = 2^{16} + 1 = 65537$?
7. Factor 831,802,500 using trial division.
8. Let the RSA primes be $p = 11$ and $q = 13$. Construct and list all possible RSA parameters $(n, \phi(n), e, d)$ using these primes.
9. Let an RSA public key system be determined by the parameters

   $$(e, n) = (37, 2953401912753470184385527395089)$$

   Given the following two messages and their signatures

   $$\begin{aligned} (M_1, S_1) &= (123456787654321, 2529045382792077409201907200017) \\ (M_2, S_2) &= (876543212345678, 1783412625941219914738123477721) \end{aligned}$$

   obtain signatures for the following messages by applying forging:

   $$\begin{aligned} M_3 &= 108215209236396770461822374638 \\ M_4 &= 2289000134448567813784851259005 \\ M_5 &= 1970129874192430866971371299001 \\ M_6 &= 1440262305070617466187763812276 \end{aligned}$$