Cryptography Homework on RSA

1. Use n, e and d from the last homework. Suppose that you try random a to factor n. Try 100 random a's. How many of them allow you to factor n? Estimate the probability of success.

2. Examine the certificates of your browser, and find the RSA public key n and e (in decimal) for `https://www.google.com`.

3. Suppose that we decide to use $e = 65537$ as the RSA public exponent. Can we use prime numbers that are congruent to $1 \pmod{e}$ to generate n? Why? Find a prime p satisfying:

   - $p \equiv 1 \pmod{e}$;
   - $2^{1000} \leq p \leq 2^{1004}$;
   - The first 9 decimal digits of p is your ID number.

   Explain your approach.