1 Introduction to Cryptography: HMW 1

1. Prove that $n^5 - n$ for positive n is always divisible by 30
2. Prove that $(p-1)! = -1 \bmod p$ for any prime p.
3. Find the smallest non-negative integer x such that

$$\begin{aligned} x &= 2 \bmod 3 \\ x &= 3 \bmod 5 \\ x &= 4 \bmod 11 \\ x &= 5 \bmod 16 \end{aligned}$$

4. Let N be an extremely large secret integer used to launch nuclear missiles. Suppose you have a commanding general and m different lieutenant generals. In the case that commanding general is incapacitated, you want each lieutenant generals to have enough partial information about N so that any three of them can agree to launch the missiles (but any one or two of them should not)

   Let $p_1, \ldots, p_m$ be m different primes, all of which are greater than $N^{\frac{1}{3}}$ but smaller than $\sqrt{N}$. Using p_i, describe the partial information about N that should be given to the lieutenant generals.

5. Calculate $38^{75} \bmod 103$ using repeated squaring method. Show every execution step of the algorithm.
6. Calculate $3125^{-1} \bmod 9987$ using extended Euclidean Algorithm. Show each step clearly.
7. Prove that DES decryption can be done by applying DES encryption algorithm to ciphertext with the key schedule reversed.
8. Bellare-Rogaway Book: Problem 2.1
9. Bellare-Rogaway Book: Problem 2.4
10. Bellare-Rogaway Book: Problem 2.6