Assignment 5
Blockchain, Cryptocurrencies and Cryptography
Due: November 27th, 2019 at the end of class.

For any doubts or queries regarding assignment please attend office hours on Monday 9:30-10:30 in CIWW 412. The assignment can we written or typed. Please write your name and netID on the assignment.

1. In cryptography, a *zero-knowledge proof* or **zero-knowledge protocol** is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. The essence of a zero-knowledge proof is that it is trivial to prove that someone possesses knowledge of certain information by simply revealing it. The challenge is to justify such possession without revealing the information itself or any additional information.
   For more about Zero Knowledge proofs :
   https://www.altoros.com/blog/zero-knowledge-proof-improving-privacy-for-a-blockchain/

   You have a special toy that has two buttons. Both buttons make different sounds when pushed. Your friend collects special toys but does not believe that your special toy makes two different sounds. He is adamant that both buttons produce the same sound. How will you convince him or with high probability prove to him that the two buttons make different sounds?

   Note: This is a Zero Knowledge proof as your friend does not know the sounds the two buttons produce, He will just know that they are different.

2. You and your friend decide to compete to carry out a 51% attack on a blockchain.
   On day 1 you acquire 1 unit of computing power. Every night you double your computing power.
   On the other hand your friend starts with 0 units on day 1 and acquires 100 additional units of computing power every night.

   In the following days, on day x-1 before either of you have enough control over the total hashrate/computing power your friend decides to dropout and sells all his cumulative computing power to you. You find that on the night of day x, you double your total computing power and realise that you finally become eligible for a 51% attack on day x.

Assume that the blockchain starts with 1000 units of computing power on day 1. Every night it increases by only 20% despite you and yours friends constant acquiring. Find Day x, the day you finally are eligible for a 51% attack.

Example: If your friend sells on Day x = 3, you will have 1 + 1 + 2 computing power. Your friend will have 0 + 100 + 100 computing power. Finally you will have 2 x 204 = 408 units of computing power on Day 4. But the total computing power in the blockchain is 1728 units on Day 4.

Write a program or calculate mathematically to find the answer.
If you programmed it (recommended), please write or print the code and clearly state the day, amount of computing power and percentage of control.

Example: If Answer was Day 4 like the example before, output is as follows:
Day = 4, Amount under control = 408 units, Percentage = (408/1728) x 100 = 23.6111%
But clearly it is not correct as you will not have eligibility to carry out a 51% attack.

Note: Although it is called a 51% attack, if you have any amount greater than 50% you are eligible to carry out the 51% attack.

3. Consider the following key:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

How would you encrypt “howareyou” with the function:
$e(x) = 5x + 7 mod 26$?

4. In order to verify a signature, do we need public and private keys? Explain your answer.