1. Assume H(.) is a collision-resistant hash function and gives out hashes of length n. Is the following clause true?
"for any x & x' that x≠x', we may conclude that H(x)≠H(x')"
Briefly describe why or why not.

2 – By using the birthday paradox, prove that the strength of a strong collision-resistant hash function is $2^{n/2}$ (i.e. the number of points we have to try to find two colliding hashes with a probability of greater than $\frac{1}{2}$).

Hint: use $e^x \approx 1 + x$ approximation if necessary

3. Let $\pi(.)$ be a permutation over the integers $0,1,2,\ldots,(2^n - 1)$. Fixing the key, DES is such a permutation for n=64. We say π has a fixed point if $\pi(m) = m$ for some m. As you might guess, it's very dangerous that a plain-text identically appears in the cipher-text. We are interested in the probability that π has no fixed points. Show that more than 60% of possible mappings will have at least one fixed point.

Hint: use inclusion-exclusion principle available at
http://www.math.umn.edu/~garrett/crypto/Overheads/06_perms_otp.pdf

4- Consider a block cipher whose block length is n. $N = 2^n$ is number of possibilities. Imagine we have t plain text-cipher text pairs { P_i, $C_i = E_K(P_i)$ } , where the key K selects one of the $N!$ Possible mappings. Now, imagine you want to brute force this encryption algorithm for the key. In each try, you generate the test key K' and check whether $C_i = E(K', P_i)$; i=1,…,t. If K' maps P_i to its proper C_i, we have an evidence that $K' = K$. However, it could be the case that $E_K(.)$ and $E_{K'}(.)$ exactly map the t given plain-texts to the same set of cipher-texts but map the other inputs differently.

a) what's the probability that $E_K(.)$ and $E_{K'}(.)$ are distinct mappings?

b) what's the probability that $E_K(.)$ and $E_{K'}(.)$ agree on another t' plain-text cipher-text pairs where $0 \leq t' \leq N - t$.

Hint: you may use the previous question's answer.

5. By definition, $\phi(n)$ is the number of natural numbers smaller or equal to n which don't have any common factor with n (i.e. their greatest common divisor (gcd) is 1).

a) prove that $\phi(pq) = (p-1)(q-1)$ if p and q are prime numbers.

b) Prove that $a^{\phi(p)} \overset{p}{\equiv} 1$ if gcd(a,p)=1. This is Fermat's little theorem. You may search for it.

c) Now, using b, prove that $a^n \overset{p}{\equiv} a^{n \bmod \phi(p)}$ if gcd(a,p)=1. Can you explain how this helps in calculating $a^x mod\ n$ for big values of x? This theory is especially useful for RSA if p is generalized to pq.