Homework 3

- Questions from Lecture unit 3
- Please refer to the lecture slides for more information about the context in which the questions arise.
- Due date: Monday, September 30, 2019

Questions

1. Public-key encryption methods,such as RSA, are much less efficient than private key encryption methods such as DES. To encrypt large messages private-key methods are preferred, but key establishment is an issue. Say Alice wants to send encrypted messages to Bob using a block-cipher (such as DES). She needs to let Bob know the key she will be using to encrypt the data. Describe how she can securely send the key to Bob by using a public key system such as RSA.

2. Prime number theorem says that as $n \to \infty$, the density of primes $\frac{\{x : x < n, n \text{ is prime}\}}{\{x : x < n\}} \sim \frac{1}{\log n}$. In other word, primes are abundant! Why is this theorem important for RSA system to be applied in practice. What else needs to be true in order for RSA to be practical?

3. Consider a normal hash function such as $h(x) = x \mod N$ where N is say a 64-bit integer. This function takes a bit string x as the binary representation of a number (for example the bit string 0010000 is identified with the number 16), then compute $x \mod N$, which is 64-bit long, as the hash. Is it secure to use this hash function in the hash-and-sign signature scheme, instead of a cryptographic hash?