COM-301 Computer Security
Exercise sheet: Applied Cryptography

1. Assume an OTP-like encryption with a short key of 128 bit. This key is then being used periodically to encrypt large volumes of data. Describe how an attack works that breaks this scheme.
2. In CTR, do you need a new Initialization Vector for every message?
3. Alice wants to have confidentiality for messages in her system. Which primitive does she need to design and implement?
4. What can you say about the:
   - Propagation of bit errors
   - Parallelizability

   for CTR and CBC modes
5. Which symmetric encryption is suitable for following scenarios? Justify.
   (a) A TV station wants to encrypt the premium live channels.
   (b) A message that can tolerate errors in a few bits is sent through a noisy channel.
   (c) A video channel wants to let users start watching from any arbitrary moment.
   (d) The sender wants to encrypt a photo.
6. A cryptographic hash function h takes as input a message of arbitrary length and produces as output a hash value of fixed length, for example 160 bits. Certain properties should be however satisfied:
   (a) Given a message m, the hash value $h(m)$ can be calculated very quickly.
   (b) Given a hash value y, it is computationally infeasible to find an m with $h(m) = y$ (in other words, h is a one-way, or first pre-image resistant function).
   (c) It is computationally infeasible to find messages m_1 and m_2 with $h(m_1) = h(m_2)$ (remember, the function h is said to be collision-free).

Let n be a large integer. Let $h(m) = m \bmod n$ be regarded as an integer between 0 and $n-1$. Argue that h satisfies (a) but not (b) and (c).

7. Bob and Alice share a secret key and use a Message Authentication Code (MAC) to authenticate messages. Bob sends a message to Alice along with its MAC. Later, Bob denies having sent the message.

   (a) Can Alice prove to a third party that Bob sent the message? Why or why not?

   (b) Would using a digital signature instead of a MAC solve this problem? Explain.