Solutions to Homework Assignment # 11

1. (a) Differential and linear cryptanalysis. Both attacks require a very large number of plaintext-ciphertext pairs encrypted under the same key. If the key is changed before the required amount of plaintext-ciphertext pairs can even be generated, the attacks become infeasible.

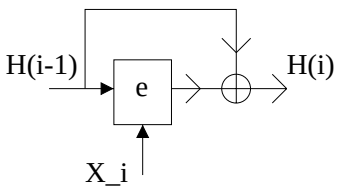
   (b) According to the estimations by Lenstra/Verheul, breaking a 1024 bit DL system is considerably easier than breaking 3DES. Hence, Oscar's best bet is to break D-H key exchange by computing a DL (**Note:** This is still infeasible right now.)

   (c) Yes, with these parameters, the key derivation approach makes sense. A D-H key exchange with 2048 bits is believed to be very secure, whereas 56 bit DES can be broken with some effort. By applying frequent key derivations, an attacker has to perform multiple key searches.

2. (a) $t = 10^6 bits/sec$
   $storage = t \cdot r = 2h \cdot 10^6\ bits/sec = 2 \cdot 3600 \cdot 10^6 bits/sec = 7.2\ Gbits = 0.9\ GByte$
   Storage of less than 1 GByte can be done at moderate costs, e.g., on hard disks or CDs.

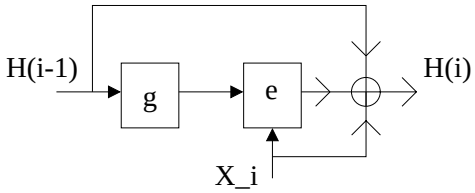
   (b) Compute # keys that an attacker can recover in 30 days:
   $\#\ Keys = \frac{30\ days}{10\ min} = \frac{30 \cdot 24 \cdot 60}{10} = 4320$
   Key derivation period:
   $T_{Kder} = \frac{2h}{4320} = 1.67\ sec$
   Since hash functions are fast, a key derivation can easily be performed (in software) at such a rate.

3. (1)



   There is no mapping function g required since there are only k bits of x fed into the encryption function, where k is the bit length of the key.

(2)



4. Attacks against hash function based on the birthday paradox are not applicable here, because Oscar can not search for an x_i such that

$$MAC_k(x_i) = MAC_k(x)$$

because he does not know k. Note that these collision–search attacks only work against hash functions, because the functions are known and do not have keys.

5. (a) If a message from Alice to Bob is found to be authentic, i.e., in fact originated from Alice, integrity is automatically assured, since an alteration by Oscar would make him the originator. However, this can't be the case if sender authenticity is assured.

   (b) No, a message can still be unaltered but message authenticity is not given. For instance, Oscar could maskerade as Alice and send a message to Bob saying that it is from Alice. Although the message arrives unaltered at Bob's (integrity is thus assured) sender authenticity is not given.

6. (a) $c_i = z_i \bigoplus \{x_1 x_2 \ldots x_n \| H_1(x) H_2(x) \ldots H_m(x)\}; \qquad i = 1, 2, \ldots, n+m$

   1) Assume x has n bits. Oscar first computes
   $z_i = x_i \oplus c_i; \qquad i = 1, 2, \ldots, n$
   2) Oscar recomputes $H(x)$ since he knows x.
   3) Assume $H(x)$ has m output bits. Oscar computes
   $z_{j+n} = H_j(x) \oplus c_{j+n} \qquad j = 1, 2, \ldots, m$
   4) Oscar computes $H(x')$
   5) Oscar computes
   $c'_i = z_i \oplus x'_i \qquad i = 1, 2, \ldots, n$
   $c'_{j+n} = z_{j+n} \oplus H_j(x') \qquad j = 1, 2, \ldots, m$

   (b) No. Although Oscar can still recover $z_1, z_2, \ldots, z_n$, he can not recover the bit-stream portion $z_{n+1}, z_{n+2}, \ldots, z_{n+m}$ which was used for encrypting $MAC_{k_2}(x)$. Even if he would know the whole bit-stream, he would not be able to compute a valid $MAC_{k_2}(x')$ since he does not know k_2.