Rob Hanlon
HW #2

1. About chosen-plaintext and chosen-ciphertext!
    a. Any situation in which the key size of a symmetric cipher is reasonably small; DES for example.
    b. Any scenario in which the adversary need only know the decrypted form of a certain message – for instance, a situation where a user's personal information is encrypted, and only this particular user's information is needed.

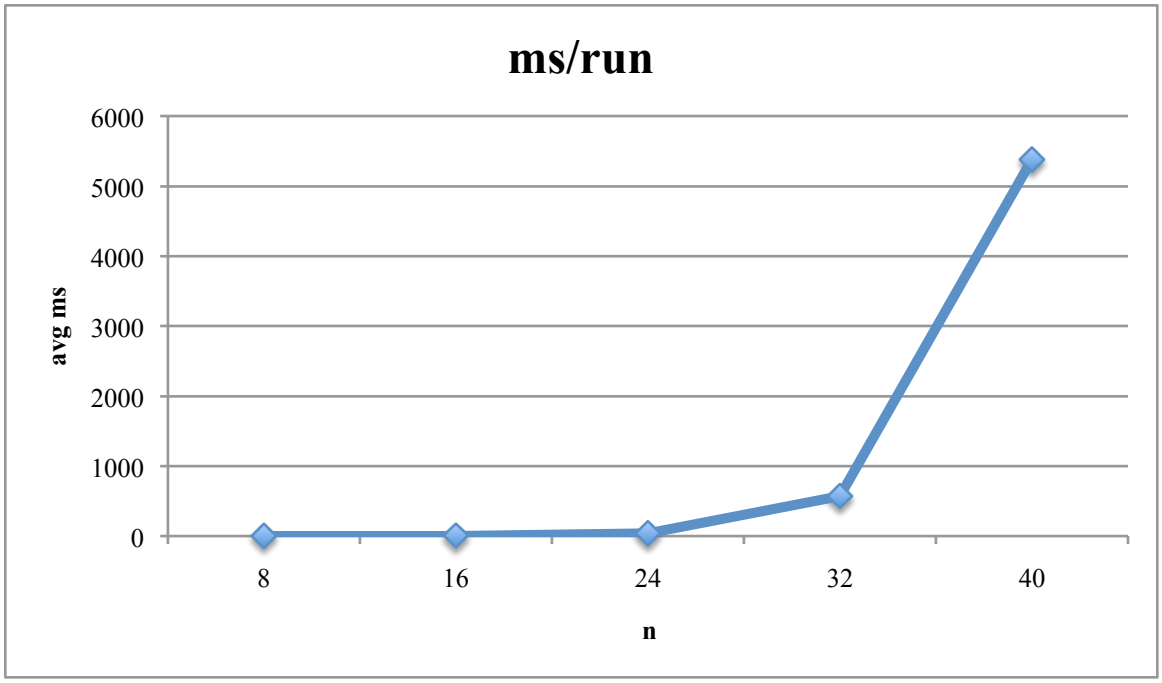
2. No, an attacker could have obtained access to Alice's secret signing key using some alternate means (e.g. gotten physical access to Alice's machine, sniffed a network connection when Alice accidentally sent her key in the clear, etc.), and then said attacker could have signed the message that Bob received with Alice's key.

3. On a processor that takes 2^{-26} seconds to perform a single DES decryption, it will take $C1' = C2$ -> , or approximately 2.98×10^5 hours. On a collection of 2^{14} processors, assuming that each processor is working at full capacity, that number drops to approximately 18.2 hours.

4. `7e 98 54 5e 43 c1 b8 b0 40 1e b8 4e a0 77 78 50`

5. C1' = C2
   C1' = blkcph(C0' ⊕ P1')
   C2 = blkcph(C1 ⊕ P2)
   blkcph(C0' ⊕ P1') = blkcph(C1 ⊕ P2)
   C0' ⊕ P1' = C1 ⊕ P2
   P1' = C1 ⊕ P2 ⊕ C0'

6. Since we have the P, and we know that both C and C' were generated using the same nonces, then we can recover the encrypted nonce + counter values and thus recover P'. We can do this by XORing each block of P with its corresponding block in C. This gives an ordered set of all the encrypted nonce + counter values; call this set N. Then, we can XOR each item in N with its corresponding block in C'. Due to the properties of XOR (A ⊕ B = C -> C XOR B = A), we thus recover each block in P'.

7. 

Due to an issue where Java was not correctly calculating SHA-512 hashes on lab machines, I ran these benchmarks locally (3.06 GHz Core 2 Duo w/ 4 GB RAM). Load averages: 0.27, 0.40, 0.46.

Pretending now that we have unlimited memory, we can very clearly see an exponential increase in the amount of time needed to find collisions as the amount of bits increase. This base of the exponential is approximately 1.22, so SHA-512-256 would require 4.05×10^{11} years, SHA-512-384 would require 4.59×10^{22} years, and SHA-512 itself would take 5.19×10^{33} years. One might consider these timespans infeasibly large…

(output is attached)

8. `be 48 c6 59 ee 04 1e dc 12 af 8d 47 96 07 76 18 99 02 e0 11 b1 c6 a5 40 56 a5 b1 0d 96 18 fa 4a`

9. M(A) = blkcph(A)
   M(B) = blkcph(B)
   M(A||B) = blkcph(blkcph(A) ⊕ B)
   M(B||(M(B) ⊕ M(A) ⊕ B)) = blkcph(blkcph(B) ⊕ blkcph(B) ⊕ blkcph(A) ⊕ B)
   = blkcph(blkcph(A) ⊕ B)
   = M(A||B)