ECE: Advanced Information and Network Security
Homework 3
Fall 2012

1. In a family of four, what is the probability that no two people have birthdays in the same month? (Assume all months have equal probabilities.)

2. Show that if someone discovers the value of k used in the ElGamal signature scheme, then a can also be determined.

3. Alice has generated an RSA public (n_A, e_A) and private key (p, q, d_A), where $n_A = pq$. Alice has signed the messages m_1 and m_2, yielding signed documents (m_1, s_1) and (m_2, s_2). Explain how Eve could use this information to sign the documents m^{-1} and $m_1 m_2$.

4. Explain how hash functions can improve the operation of digital signatures. What properties of hash functions are necessary in order for "signing the hash" to be a secure technique? Finally, explain how "signing the hash" protects against existential forgery attacks on digital signatures? (In explaining your answer, assume RSA signatures with message m and hash function h()).