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.)

Solution: The probability that no two have birthdays in the same month is

$$(1 - 1/12)(1 - 2/12)(1 - 3/12) = 165/288$$

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

Solution: If Eve discovers k, then she can use r, s, m to write $ar = m - ks(modp - 1)$ and solve for a. There will be gcd(r, p - 1) solutions for a. This will probably be a small number. Each of these possible values a can then be tested until one is found that satisfies $\beta = \alpha^a \pmod{p}$.

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 $m_1 m_2$.

Solution: Simply invert s_1 and multiply s_1 with s_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()).

Solution: See book/notes for the desirable properties. You sign the hash of the message to make a message with appendix of the form $[m, sig_A(h(m))]$. Signing the hash prevents existential forgery since it is impossible for an adversary to create another message whose hash is controlled in a manner that would produce a meaningful signature.