CS 355, Fall, 2019, Homework 8

1. There is a flaw in the key exchange protocol of Denning and Sacco. Suppose Alice and Bob have a brief secret conversation, so that the time stamp t_A is still valid when they finish. (a) Explain how Bob could pretend to be Alice and communicate with Carol so that Carol thought she was talking to Alice. (b) Repair this flaw with a minor change to one message.

2. Alice uses a trick to speed her RSA signature generation. Suppose her modulus is $n = pq$, where the primes p and q have about the same length. Let b be the number of bits in n, so that the length of p and q is about $b/2$ bits. If the decryption exponent is d, then Alice signs the plaintext M as $S = D(M) = M^d \bmod n$. The trick replaces this fast exponentiation with b-bit numbers by two fast exponentiations with $b/2$-bit numbers. (This makes the signature generation run about four times faster.) Let $M_p = M \bmod p$, $M_q = M \bmod q$, $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$. The length of each of these four numbers is about $b/2$ bits. Alice computes $S_p = M_p^{d_p} \bmod p$ and $S_q = M_q^{d_q} \bmod q$ by fast exponentiation. Now the signature $S \equiv S_p \pmod{p}$ and $S \equiv S_q \pmod{q}$, so Alice computes $S = D(M)$ from S_p and S_q by the Chinese remainder theorem. In the application of the Chinese remainder theorem, some numbers may be precomputed. The result is that $S = (fS_p + gS_q) \bmod n$ where f and g are precomputed constants.

Find the constants f and g.