CS 427/519: Homework 6

Due: Monday March 5, 10pm; **typed** and **submitted electronically**.

1. Let F be a secure PRP with block length λ. Suppose we use CBC-MAC with a fixed key, as a hash function. Demonstrate how to efficiently find a collision in the following H, when k is public:

   $H(m_1 \| m_2 \| m_3)$:
   $c_1 := F(k, m_1)$
   $c_2 := F(k, m_2 \oplus c_1)$
   $c_3 := F(k, m_3 \oplus c_2)$
   return c_3

2. Show that given an RSA modulus N and $\phi(N)$, it is possible to factor N easily. Use it to factor the modulus given in supplementary file `hw6.txt` (on the course website).

   Hint: you have two equations (involving $\phi(N)$ and N) and two unknowns (p and q).

3. Bob chooses an RSA plaintext $m \in \mathbb{Z}_N$ and encrypts it under Alice's public key as $c \equiv_N m^e$. To decrypt, Alice first computes $m_p \equiv_p c^d$ and $m_q \equiv_q c^d$, then uses the CRT conversion to obtain $m \in \mathbb{Z}_N$, just as expected. But suppose Alice is using faulty hardware, so that she computes a **wrong value** for m_q. The rest of the computation happens correctly, and Alice computes the (wrong) result $\hat{m}$. Show that, no matter what m is, and no matter what Alice's computational error was, Bob can factor N if he learns $\hat{m}$.

   Use this approach to factor the modulus given in supplementary file `hw6.txt` (on the course website).

   Hint: Bob knows m and $\hat{m}$ satisfying the following:

   $$m \equiv_p \hat{m}$$
   $$m \not\equiv_q \hat{m}$$

grad. Let p and q be distinct primes. Euler's thereom implies that $x^{(p-1)(q-1)} \equiv_{pq} 1$ for all $x \in \mathbb{Z}^*_{pq}$.

Use the CRT to prove the following tighter version, that $x^{\text{lcm}(p-1, q-1)} \equiv_{pq} 1$ for all $x \in \mathbb{Z}^*_{pq}$.