Cryptography: HW5

Due electronically (via TEACH) on **Friday** Feb 26

1. Submit two JPG files with your homework. One should be a picture of a cat, the other should be a picture of a dog. The MD5 hashes of the two files should agree in the first 5 bytes (= 40 bits = 10 hex digits). Describe how you obtained these files.

```
$ md5sum *jpg
d43672572a00c1474a62cea60138395d  cat.jpg
d43672572a09a8d09132d5fee2cb50cb  dog.jpg
```

   Hint: The JPG format allows arbitrary data to be added to the end of a valid JPG file.

   Note: The parameters are chosen so that 1 week is not enough time to compute an answer using the *wrong* approach. So you should probably use the *right* approach (my implementation takes a few seconds).

2. The Chinese Remainder Theorem states that there is always a solution for x in the following system of equations, when $\gcd(r,s) = 1$:

$$x \equiv_r u$$
$$x \equiv_s v$$

   Give an example u, v, r, s, with $\gcd(r,s) \neq 1$ for which the equations have no solution. Explain why there is no solution.

3. (a) Show that given an RSA modulus N and $\phi(N)$, it is possible to factor N easily. This means that if you can efficiently compute $\phi(N)$ given N, then you can factor N.

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

   (b) What are the two prime factors of the huge RSA modulus N below (see also the data file on the website)? Please submit your answer in a plaintext file.

```
  N = 114655786929363293547270171835818019983713930755936293416213692
      626890468137721622845271322721553217481206878852746865285508022
      331900979484825085984473800371529277882510871476845661023259372
      121427307888965698764455104708035399847578737685221765628332087
      185062953620862533363209440391640516716705907325781839818668922
      613012616866109863197276174478909304763951880347472829094263896
      839210949723611578356422185670462011244441099280712789830695333
      761027183159133122984776111031962562145 23

 phi = 114655786929363293547270171835818019983713930755936293416213692
      626890468137721622845271322721553217481206878852746865285508022
      331900979484825085984473800371529277882510871476845661023259372
      121427307888965698764455104708035399847578737685221697389859181
      873598549114836175107363332870527861935627438414238359599325743
      980991746581657826242781429934838034223650839090328554275002703
      153127829530332006955135657845058823676827043506907310991926628
      794434555212427008741637877609748913480 40
```