CS3235 tutorial questions for week 8
(Fri Oct 1-Thu Oct 7(!!), 2004)

September 29, 2004

1. Calculate the minimum extra bits needed for encoding a 32 bit value, with two-bit error detection. *Show your own worked version of the Hamming calculation in the notes.*

2. Calculate the minimum extra bits needed for encoding a 32 bit value, with two-bit error correction. *Show your own worked version of the Hamming calculation in the notes. Note that in this case we want to do error recovery, not error detection.*

3. In the repetition scheme for error correction, there is no point in repeating bits twice. you must repeat three times, or 5 times. Why is this?

4. Diffie-Hellman key exchange is used to exchange keys over a possibly insecure channel, where hacker Bob might be listening to the communication. Give a worked example of a Diffie-Hellman key exchange between Alice and Ted using small sized (say 3 to 5-digit) numbers[1]. Clearly show what Bob's problem is (Bob is listening to the communication between Alice and Ted and trying to discover the keys).

5. In the final step of the (RSA) proof that $c^D \bmod N$ calculates the original message m, we had

$$\begin{aligned} c^D \bmod N &= m^{ED} \bmod N \\ &= m^{k(P-1)(Q-1)+1} \bmod PQ \\ &= m * m^{k(P-1)(Q-1)} \bmod PQ \\ &= m \end{aligned}$$

and then we noted that:

$m^{P-1} \bmod P = 1$, so $(m^{(P-1)})^{k(Q-1)} \bmod P = 1$

$m^{Q-1} \bmod Q = 1$, and so (tutorial) $(m^{(P-1)})^{k(Q-1)} \bmod PQ = 1$.

Why is it that given $m^{P-1} \bmod P = 1$ and $m^{Q-1} \bmod Q = 1$ then $(m^{(P-1)})^{k(Q-1)} \bmod PQ = 1$?

[1] Of course a real exchange would use numbers with hundreds of digits. In this case Bob could discover the keys, but if the numbers had hundreds of digits...