Erikson Sodergren CS462-01

1. By testing each possible value to shift by until a plaintext message is found, the result was "IFWEALLUNITEWEWILLCAUSETHERIVERSTOSTAINTHEGREATWATERSWITHTHEIRBLOOD". This was said by Tecumseh

2. (a) 100% overhead turns the $50 into $100 each, so 10,000 parallel ASIC's can be used. This can check $5*10^{12}$ possible keys each second. 128 bit keys have 2^{128} possible keys, so the average keys we need to check to find the right one is 2^{127} or roughly $1.7*10^{38}$. Therefore an average search takes $1.7*10^{38} / 5*10^{12} = 3.4*10^{25}$ seconds = $1.08*10^{18}$ years, significantly longer than the universe has existed.
   (b) $3.4*10^{25}$ seconds = $3.94*10^{20}$ days.
   1 day= $3.94*10^{20}$ days / $2^{(months/18)}$
   $2^{(months/18)}$ days = $3.94*10^{20}$ days
   months/18 = $\log_2(3.94*10^{20})$
   Months = 18 * 68.4 = 1231 months = 102.6 years

3. (a) $128^8 = 7.2*10^{16}$ possible keys
   (b) 56 bits of key(7 bits per char, 8 chars)
   (c)26 options can be held in 5 bits, so 5*8=40 bits
   (d)(i) 128/7 = 18.2 so 19 characters
   (ii) 128/5 = 25.6 so 27 characters4