SKETCH OF SOLUTIONS (HOMEWORK XI)

1.- $5^{27} \equiv 94 \mod 103$ and $94^{31} \equiv 90 \mod 103$

6.- a) $\Phi(19 \cdot 67) = 1188$ and $(713 \cdot 5) \equiv 1 \mod 1188$. The numerical equivalents of the message are:

$$0614, 1403, 0418, 2204, 0419, 1114, 2104$$

The decryption function is raising each block to the 713th power $\mod 19 \cdot 67$. We get:

$$1100, 0731, 0945, 0304, 0285, 0324, 1046, 1248$$

Since the other modulus is smaller we split each block in two before encrypting them with the other key. The encryption function is raising each block to the 3rd power and reducing modulo $11 \cdot 71$. We get.

$$550, 000, 343, 113, 729, 529, 027, 064, 008, 259, 027, 547, 219, 492, 166, 471$$

b) Same procedure as in a) (with the appropriate keys!!) The message is:

$$000, 266, 32, 1119, 225, 442, 900, 1127, 1119, 999, 1119, 1127$$

10.- $K_0 = K + tp = 5 + 14 \cdot 7 = 103$. The three shadows are given by $k_1 \equiv 103 \equiv 4 \mod 11$, $k_2 \equiv 103 \equiv 7 \mod 12$, $k_3 \equiv 103 \equiv 1 \mod 17$

Section 9.1

1.- a)4, b) 4, c) 6, d) 4

6.- Notice that the group of units $\mod 20$ is $\{1, 3, 9, 7\} \times \{1, 19\} =< 3 > \times < 19 >$ therefore the highest order is 4

10.- Suppose $\text{ord}_n a = r$ and $\text{ord}_n b = s$. Then

$$(ab)^{rs} = a^{rs} b^{rs} = (a^r)^s (b^s)^r = 1$$

Therefore $t := \text{ord}_n(ab) \mid rs$. Also, notice that

$$1 \equiv (ab)^t \equiv (ab)^{rt} \equiv (a^r)^t b^{rt} \equiv b^{rt} \mod n$$

But this implies that $s \mid rt$, thus $s \mid t$ (since $(r, s) = 1$) Similarly $r \mid t$. Therefore $rs \mid t$. i.e. $rs = t$

18.- Let $h = \text{ord}_p 2$ Then $h \mid \Phi(p) = p - 1$. Note that $2^{2^n} \equiv -1 \mod p$, so $(2^{2^n})^2 \equiv 2^{2^{n+1}} \equiv 1 \mod p$. Therefore, $h \mid 2^{n+1}$, say $h = 2^k$. But if $k < n + 1$ then $2^{2^n} \equiv 1 \mod p$ (a contradiction. Therefore $h = 2^{n+1}$

b) Since $2^{n+1} = \text{ord}_p 2 \mid \Phi(p) = p - 1$, we have $2^{n+1} k = p - 1$ or $p = 2^{n+1} k + 1$