1.

a) $Y_a = \alpha^{x_a} \bmod 71 = 5^7 \bmod 71 = 25$
b) $Y_b = \alpha^{x_b} \bmod 71 = 5^12 \bmod 71 = 25$
c) $K_s = Y_a^{x_b} \bmod 71 = 57$
d)
$Y_a = {x_a}^{\alpha} = 7^5 \bmod 71 = 51$
$Y_b = {x_b}^{\alpha} = 7^12 \bmod 71 = 4$
$K_s = Y_b X_a^{\alpha} \bmod p = 62$ and
$K_s = Y_a X_b^{\alpha} \bmod p = 62$

2.

a) Hacker found another message with the same signature
b) $2^{64} * 64$ bits
c) $2^{32}/2^{20} = 2^{12} = 4096$ seconds
d) $2^{128} * 128$ bits $2^{64}/2^20 = 2^42$ seconds $= 139461$ years

3.

$P = 01010111$
$t_i = a * s_i \bmod p$
$t = \{1097, 1175, 1409, 1877, 1009, 1194, 779, 456\}$
$c = \sum_{i=1}^{n} t_i * P_i = 5481$
$Z = a^{-1} c \bmod p = 1589 * 5481 \bmod 1999 = 1665$
$1665 - 946 = 719$, $719 - 450 = 269$, $269 - 215 = 54$, $54 - 45 = 9$, $9 - 9 = 0$
thus $P = 01010111$