Josh Barthelmess

1.

(a) $Y_A = 7^5 \bmod 71 = 51$

(b) $Y_B = 7^{12} \bmod 71 = 4$

(c) $K = 4^5 \bmod 71 = \boxed{30}$

(d) They would be unable to create a shared key, and the secret number chosen is theoretically vulnerable

2.

(a) The attacker finds a valid message that has the same hash as his fraudulent message, obtains valid Authentication with valid message and attaches it to his fraudulent message

(b) $M \cdot 2^{32}$ ← approximate number needed to find valid match probabilistically

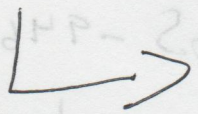
(c) $\frac{2^{32}}{2^{20}} = 2^{12}$ seconds

≈ 1.14 hours

(d)

Space: $M \cdot 2^{64}$

time: 2^{44} seconds $\approx 557{,}000$ years



(3)

$P = 01010111$ $\rho = 1999$ $a = 1019$

$S = \{5, 9, 21, 45, 103, 215, 450, 946\}$

$S_{pub} = \{a \cdot S_i \bmod \rho\} = \{1097, 1175, 1409, 1877, 1009, 1194, 779, 456\}$

a^{-1}:

0: $1999 = 1(1019) + 980$ $\rho_0 = 0$

1: $1019 = 1(980) + 39$ $\rho_1 = 1$

2: $980 = 25(39) + 5$ $\rho_2 = 1998 \bmod 1999$

3: $39 = 7(5) + 4$ $\rho_3 = 1 - 1998 = 2 \bmod 1999$

4: $5 = 1(4) + 1$ $\rho_4 = 1998 - 2(25) = 1948 \bmod 1999$

$\rho_5 = 2 - (1948) \bmod 1999$
$= 359$

$\rho_6 = 1948 - 359 = \boxed{1589}$

$C = \sum P \cdot S_{pub} =$ ~~$1097 + 1175 + 1409 + 1877 + 1009 + 1194 + 779 + 456 = 1665 \bmod 1999$~~

$1175 + 1877 + 1194 + 779 + 456 = 1483 \bmod 1999$

$C' = C \cdot a^{-1} \bmod \rho = 1665 - 946 = 719 - 450 = 269 - 215 = 54 - 45 = 9 - 9 = 0$

1 1 1 0 1 0 1 0

P: $\boxed{01010111}$