

- 1) a) $\gamma_A = 7^5 \bmod 71 = 51$
- b) $\gamma_B = 7^{12} \bmod 71 = 4$
- c) $K = 4^5 \bmod 71 = 30 = 51^{12} \bmod 71$
- d) Unable to create a shared key, and X_A is vulnerable.

2) a) generate many valid messages till he finds one with same hash as fraudulent message. Uses valid for authentication, but attaches it to fraudulent message.

- b) $M \cdot 2^{64/2} = M \cdot 2^{32}$
- c) $2^{12} \approx \boxed{1.14 \text{ hours}}$
- d) $M \cdot 2^{128/2} = M \cdot 2^{64}$
 $2^{44} \text{ sec} = 557,474 \text{ years}$

3)

$$P = 01010111$$

$$a = 1019$$

$$S = 5, 9, 21, 45, 103, 215, 450, 946 \quad Q = 1999$$

$$S_p = a S_i \bmod P$$

$$S_p = \{1097, 1175, 1409, 1877, 1009, 1194, 779, 456\}$$

$$1999 = 1(1019) + 980$$

$$1019 = 1(980) + 39$$

$$980 = 25(39) + 5$$

$$39 = 7(5) + 4$$

$$5 = 1(4) + 1$$

$$\begin{array}{c} 0 \\ 1 \end{array}$$

$$0 - 1 \bmod 1999 = 1998$$

$$1 - 1998 \bmod 1999 = 2$$

$$1998 - 2(25) \bmod 1999 = 1948$$

$$25 - 1948(7) \bmod 1999 = 359$$

$$1948 - 359 \bmod 1999 = \boxed{1589} = a^{-1}$$

$$C = \sum P \cdot S_p = (1175 + 1877 + 1194 + 779 + 456) \bmod 1999 = 1483$$

$$C' = (a^{-1} \bmod 1999) = 1665$$

$$1665 - 946 = 719$$

$$719 - 450 = 269$$

$$269 - 215 = 54$$

$$54 < 103 \quad 9$$

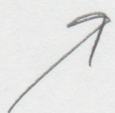
$$54 - 45 = 9$$

$$9 < 21$$

$$9 - 9 = 0$$

$$0 < 5$$

$$\begin{array}{c} 1 \\ 1 \\ 1 \\ \textcircled{1} \\ 1 \\ 0 \\ 1 \\ 0 \end{array}$$



$$\boxed{01010111}$$