Samad Farooqui 10/14/2018 HW 2.b

(a) If $X_A = 5$, $Y_a = 7^5 \bmod 71 = 51$

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

(c) The shared key is

$51^{12} \bmod 71$ or $4^{12} \bmod 71 = 58$

(d). Finding the $6^{th}$ root is easy if you know a. The reason you use, for say, $7^x \bmod 71 = 51$ is because it is hard to find the solution to the discrete log problem. You would have to do $x = \log_7 51$. In the other case the problem suggests, you would have $x^7 \bmod 71$. You could find $x = \sqrt[7]{27}$ very easily, therefore it is $x^7 \bmod 71 = 51$.

Q-2) (a). The attack is exploiting the probability that two values hash to the same hash value. The attacker would be trying a bunch of values that he can generate, and if any are valid, the attacker can send it to a client and the client would think it is valid.

$2^{\frac{m}{2}}$

(b). It is a 64-bit hash code, so $2^{\frac{m}{2}}$ is the space required. Therefore, it is $2^{32} \cdot 64$ as there are 64 bit messages. So, is $2^{32}$ to try everything, and store it, and the 64 ($2^6$) for each try.

(c) $2^{32}$ ~~hashes~~ $\times \frac{1 \text{ second}}{2^{20} \text{ hashes}} = \frac{2^{32}}{2^{20}} = 2^{12}$ seconds

$= 4096$ seconds.

(d) $2^{\frac{128}{2}} = 2^{64}$ hashes $\cdot 2^6$ so around space for $2^{70}$ bits

The time needed to compare hashes is

$2^{64} \text{ hashes} \times \frac{1 \text{ second}}{2^{20} \text{ hashes}} = 2^{44}$ seconds, which is

557845 years. Wow!

Q3) $1019 \cdot 5 \bmod 1999 = 1097$

$1019 \cdot 9 \bmod 1999 = 1175$

$1019 \cdot 21 \bmod 1999 = 1407$

$1019 \cdot 45 \bmod 1999 = 1877$

$1019 \cdot 103 \bmod 1999 = 1009$

$1019 \cdot 215 \bmod 1999 = 1194$

$1019 \cdot 450 \bmod 1999 = 779$

$1019 \cdot 946 \bmod 1999 = 456$

The inverse $a^{-1} \bmod p$ is equal to $a^{p-2} \bmod p$ by Fermat's little theorem, which is $1019^{1997} \bmod 1999 = 1589$ by Wolfram Alpha

| 1097 | 1175 | 1407 | 1877 | 1009 | 1194 | 779 | 456 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

$1175 + 1877 + 1194 + 779 + 456 = 5481 = W$

We figure out the plaintext by doing

$a^{-1} \cdot W \bmod p$

$= 1589 \cdot 5481 \bmod 1999 = \boxed{1665 = P}$

This instance was solved with the following instruction: Solve the Instance $I = (S, C)$ of subset sum problem to obtain the plaintext.