Jack Phillips
Crypto p3

Q1) $q = 71$ $\alpha = 7$

a) $X_A = 5$ $Y_a = 7^5 \bmod 71 = \boxed{51}$

b) $X_B = 12$ $Y_b = 7^{12} \bmod 71 = \boxed{4}$

c) Shared secret:

$S = (Y_a)^{X_B} \bmod 71 = \boxed{30}$ $S = (Y_b)^{X_a} \bmod 71 = \boxed{30}$

d) Diffie helman is based off this property:

$(\alpha^a \bmod p)^b \bmod p = \alpha^{ab} \bmod p$

Therefore if you sent (α^α) you are invalidating they system. Also if it did work you make it unsafe because you remove the descreat log.

Q2)

a) The idea here is you generate a bunch of valid and invalid packets and keep going till you have a valid packet that colids with an invalid one. Now you can get a signature for both, It works because when you try to colide with on hash it is supper rare, but the change that two hash in the group will be the same is much more likly. The principal of the Birthday Problem

b) for $\to 50\%$ chance you make:

c) $2^{hs/2} + 2^{hs/2}$ hs = hash size = 64 bits

then m size: $\boxed{m \cdot 2^{32} + m \cdot 2^{32}}$

c) so they need to fine $2^{32} + 2^{32}$ hashes:

it's $\dfrac{2^{32} + 2^{32}}{2^{20}} = \boxed{8192 \text{ Sec}}$

d) when 128 it's
$m \cdot 2^{64} + m \cdot 2^{64}$ space
and

$$\frac{2^{64} + 2^{64}}{2^{20}} = \boxed{35184372088832 \text{ sec}}$$

A lot longer ∴ 2^{45}

Q3) generate key! "0101 0111"

$B_i = aS_i \bmod p$

$B_1 = 1019 \cdot 5 \bmod 1999 = 1097$

$B_2 = 1019 \cdot 9 \bmod 1999 = 1175$

$B_3 = 1019 \cdot 21 \bmod 1999 = 1404$

$B_4 = 1019 \cdot 45 \bmod 1999 = 1877$

$B_5 = 1019 \cdot 103 \bmod 1999 = 1009$

$B_6 = 1019 \cdot 215 \bmod 1999 = 1194$

$B_7 = 1019 \cdot 450 \bmod 1999 = 779$

$B_8 = 1019 \cdot 946 \bmod 1999 = 456$

Encrypt:

$C = 0 + 1(1175) + 0 + 1(1877) + 0 + 1(1194) + 1(779) + 1(456) = \boxed{5481}$

decrypt: $a^{-1} = a^{m-2} \bmod p$ cool rule

$a^{-1} = 1589$

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

$1665 - 946 = 719$

$719 - 450 = 269$

$269 - 215 = 54$

$54 - 45 = 9$

$9 - 9 = 0$

$$\begin{array}{cccccccc} 5 & 9 & 21 & 45 & 103 & 215 & 450 & 946 \\ \end{array}$$

Number is $\boxed{0\ 1\ 0\ 1\ 0\ 1\ 1\ 1}$

It worked ✓