P G

Q1 Common prime = 71 primitive root 7

a) User A has a private key $X_a = 5$, find public key

$A = 7^5 \bmod 71 = 51$

b) user B has a private key $X_B = 12$ find public key

$B = 7^{12} \bmod 71 = 4$

c) Shared secret key

$S = 4^5 \bmod 71 = 30$

$S = 51^{12} \bmod 71 = 30$

d) $5^7 \bmod 71 = 25$

$12^7 \bmod 71 = 25$

$S = 25^5 \bmod 71 = 1$

$S = 25^{12} \bmod 71 = 57$

So with our above example we can no longer guarantee that the calculated shared key is the same

Q2

A) Our has been attempting to create a fraudulent where it's checksum value obtained from the hash function is the same as an original non-dangerous message. If the ~~A~~ signatured recieved is valid aka checksum of fraudulent message is equal to the checksum of the valid message, then the birthday attack has succeeded and the fraudulent message can be sent.

B) For an M-bit message the attacker needs $2^{m/2}$ bits. This is because a hash function generates 2^m outputs, but due to the birthday paradox it takes $2^{m/2}$ instead of 2^m.

C) $\frac{2^{64/2}}{2^{20}} = 2^{32}/2^{20} = 2^{12} = 4096$ seconds
or about 68.26 minutes.

D) use 128 bit hash
(B) attacker needs $2^{128/2} = 2^{64}$ bits

(C) $2^{64}/2^{20} = 2^{44}$ seconds = 565,592.4 years

Q3 ciphertext = 0101 0111

$a = 1019$, $p = 1999$

$S = \{5, 9, 21, 45, 103, 215, 450, 946\} = 1794$

- is $p >$ than ΣS yes $1999 > 1794$

is gcd $(1999, 1019) = 1$? yes

$1999 \equiv 1019 \times 1 + 980$
$1019 \equiv 980 \times 1 + 39$
$980 \equiv 25 \times 39 + 5$
$39 \equiv 7 \times 5 + 4$
$5 \equiv 4 \times 1 + 1$
$4 \equiv 4 \times 1 + 1$ gcd of 1

- So a & p are coprime.

$\beta = \{(5 \times 1019) \bmod 1999 = 1097$
$(9 \times 1019) \bmod 1999 = 1175$
$(21 \times 1019) \bmod 1999 = 1409$
$(45 \times 1019) \bmod 1999 = 1877$
$(103 \times 1019) \bmod 1999 = 1009$
$(215 \times 1019) \bmod 1999 = 1194$
$(450 \times 1019) \bmod 1999 = 779$
$(946 \times 1019) \bmod 1999 = 456$

$C = [1097 \cdot 0] + [1175 \cdot 1] + [1409 \cdot 0] + [1877 \cdot 1]$
$+ [1009 \cdot 0] + [1194 \cdot 1] + [779 \cdot 1] + [456 \cdot 1]$

$C = 5481$

$5481 \cdot 1589 \bmod 1949 = 1665$

$1665 - 946 = 719$
$719 - 450 = 269$
$269 - 215 = 54$
$54 - 45 = 9$
$9 - 9 = 0$

check elements of 1 bit for private key
we get: 0101 0111 which is correct.