Cavell Teng
Cryptography
HW 2.6.

Q1. (a) $q = 71$ & $\alpha = 7$ $\quad X_A = 5$

$Y_A = 7^{X_A} \bmod 71 = 51$

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

(c) Shared Key : $Y_B^{X_A} \bmod 71 = Y_A^{Y_B} \bmod 71 = 30$

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

$Y_B = 12^7 \bmod 71 = 25$

shared key : $Y_B^{X_A} \bmod 71 : Y_A^{Y_B} \bmod 71$

$25^5 \bmod 71 = 1$

$25^{12} \bmod 71 = 57$ } Not equal

Cannot guarantee that calculated shared key is the same.

Q2. (a) The attacker has been attempting to generate a fraudulent message that generates a check sum that is the same as an original one. If the signature received is valid, where the check sum of the valid is equal to that of the fraudulent message, the attacker can now send fraudulent messages posed as real ones.

(b) For an M-bit message, the attacker $2^{\frac{M}{2}}$ bits is the approximate amount needed.

(c) $2^{64} \rightarrow 2^{32}$ security

$\frac{2^{32}}{2^{20}} = 2^{12}$ seconds $= 4096$ seconds $= 68.2\overline{6}$ minuts

(d) $2^{128} \rightarrow 2^{64}$ security (b)

$\frac{2^{64}}{2^{20}} = 2^{44}$ seconds ≈ 565592.4 years

Q3. $P = '0101\ 0111'$

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

$a = 1014$, $p = 1999$

$p > \sum S \rightarrow 1999 > 1794$

$\gcd(1999, 1014) = 1$ * work is next page

a & p are co-prime

$1999 = 1019(1) + 980$

$1019 = 980(1) + 39$

$980 = 39(25) + 5$

$39 = 5(7) + 4$

$5 = 4(1) + 1$

$4 = 1(4) + 0$ gcd of 1.

$\beta = \{ (5 \times 1019) \bmod 1999 = 1097, \quad 0$

$(9 \times 1019) \bmod 1999 = 1175, \quad 1$

$(21 \times 1019) \bmod 1999 = 1409 \quad 0$

$(45 \times 1019) \bmod 1999 = 1877, \quad 1$

$(103 \times 1019) \bmod 1999 = 1009, \quad 0$

$(215 \times 1019) \bmod 1999 = 1194 \quad 1$

$(450 \times 1019) \bmod 1999 = 229 \quad 1$

$(946 \times 1019) \bmod 1999 = 456 \quad 1$

$\downarrow$

$c = 5481$

Inverse modulo $1019 \bmod 1999$

$5481 \times 1589 \bmod 1999 = 1665$

$1665 - 946 = 719$ ✓

$719 - 450 = 269$ ✓ Same as 1's bit places

$269 - 215 = 54$ ✓

$54 - 45 = 9$ ✓

$9 - 9 = 0$ ✓