The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 10 Workshop – 16th and 17th May 2019

1. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 157$ and a primitive root $\alpha = 5$.

   a. If Alice has a private key $XA = 15$, find her public key YA.
   b. If Bob has a private key $XB = 27$, find the public key YB.
   c. What is the shared secret key between Alice and Bob?

2. Solve the following problem, now as Birthday Paradox, and use the solution to analyse the Birthday Attack on a hash function.

Birthday Paradox: What is the minimum value of k such that the probability is greater than 0.5 that at least two people in a group of k people have the same birthday?

3. Prove that in DSA signature verification we have $v = r$ if the signature is valid.

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \le L \le 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p - 1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (\mathrm{H}(M) + xr)] \bmod q$

Signature = (r, s)

Verifying

$w = (s')^{-1} \bmod q$

$u_1 = [\mathrm{H}(M')w] \bmod q$

$u_2 = (r')w \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

M = message to be signed
$\mathrm{H}(M)$ = hash of M using SHA-1
M', r', s' = received versions of M, r, s

Figure 13.4 The Digital Signature Algorithm (DSA)