The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 11 Workshop – 17th and 19th May 2021

Solutions

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

a. If Alice has a private key X_A= 15, find her public key Y_A.
b. If Bob has a private key X_B = 27, find the public key Y_B.
c. What is the shared secret key between Alice and Bob?

Solution:

a. $Y_A = 5^{15} \bmod 157 =$
$= 5 \times 5^{14} \bmod 157$
$= 5 \times 25^{7} \bmod 157$
$= 5 \times 25 \times 25^{6} \bmod 157$
$= 125 \times (25^2)^3 \bmod 157$
$= 125 \times (625)^3 \bmod 157$
$= 125 \times (154)^3 \bmod 157$
$= 125 \times 154 \times (154)^2 \bmod 157$
$= 96 \times (154)^2 \bmod 157$
$= 96 \times 9 \bmod 157$
$= 96 \times 9 \bmod 157$
$= 79$

b. $Y_B = 5^{27} \bmod 157$
$= 5 \times 5^{26} \bmod 157$
$= 5 \times 25^{13} \bmod 157$
$= 5 \times 25 \times 25^{12} \bmod 157$
$= 125 \times (25^2)^6 \bmod 157$
$= 125 \times 154^6 \bmod 157$
$= 125 \times (154^2)^3 \bmod 157$
$= 125 \times 9^3 \bmod 157$
$= 125 \times 9 \times 9^2 \bmod 157$
$= 26 \times 81 \bmod 157$
$= 65$

c. $K = 5^{15\times 27} \bmod 157$
$= 5^{405} \bmod 157$
$= 5 \times 5^{404} \bmod 157$
$= 5 \times (5^2)^{202} \bmod 157$
$= 5 \times 25^{202} \bmod 157$
$= 5 \times (25^2)^{101} \bmod 157$

$$
\begin{aligned}
&= 5 \times 154^{101} \bmod 157 \\
&= 5 \times 154 \times 154^{100} \bmod 157 \\
&= 142 \times (154^2)^{50} \bmod 157 \\
&= 142 \times\ 9^{50} \bmod 157 \\
&= 142 \times (9^2)^{25} \bmod 157 \\
&= 142 \times 81^{25} \bmod 157 \\
&= 142 \times 81 \times 81^{24} \bmod 157 \\
&= 41 \times (81^2)^{12} \bmod 157 \\
&= 41 \times 124^{12} \bmod 157 \\
&= 41 \times (124^2)^{6} \bmod 157 \\
&= 41 \times 147^{6} \bmod 157 \\
&= 41 \times (147^2)^{3} \bmod 157 \\
&= 41 \times 100^{3} \bmod 157 \\
&= 41 \times 100 \times 100^{2} \bmod 157 \\
&= 18 \times 109 \bmod 157 \\
&=\ 78
\end{aligned}
$$

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

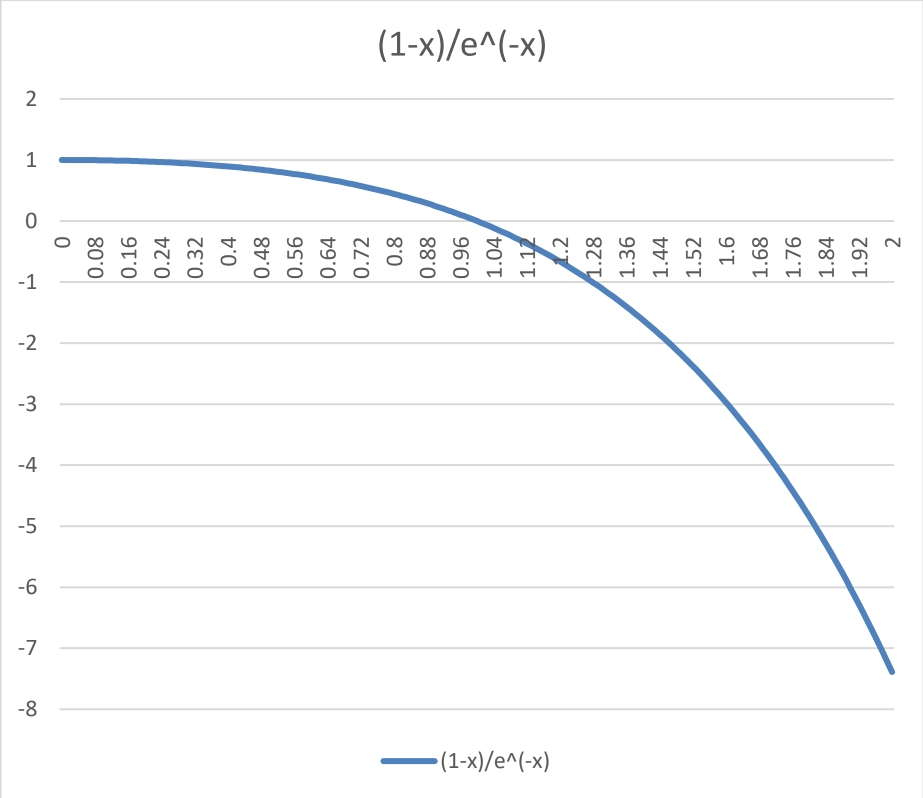
Birthday Paradox: What is the minimum value of k such that the probability is greater than 0.5 that at least 2 people in a group of k people have the same birthday?

Solution: We will ignore 29 Feb and assume that all birthdays are equally likely. The number of ways in which k people can have all different birthdays is 365×364×…×(365-k+1) and the total number of ways in which k people can have birthdays is 365^k. This the probability that k people all have different birthday is $\frac{365!}{(365-k)!365^k}$, thus the probability that at least 2 have the same birthday is $1 - \frac{365!}{(365-k)!365^k}$.

In general, if we consider n instead of 365, such that k ≤ n we have $P(n,k) = 1 - \frac{n!}{(n-k)!n^k}$

To evaluate this expression we will use the following approximation: $(1-x) \le e^{-x}$, and $(1-x)\ \approx\ e^{-x}$ for small x.

What does "small x" mean? The following graph shows $\frac{1-x}{e^{-x}}$ which should be close to 1.



We have

$$P(n,k) = 1 - \frac{n!}{(n-k)!\,n^k} = 1 - \frac{n-1}{n} \times \frac{n-2}{n} \times \ldots \times \frac{n-k+1}{n}$$

$$= 1 - \left(1 - \frac{1}{n}\right) \times \left(1 - \frac{2}{n}\right) \times \ldots \times \left(1 - \frac{k-1}{n}\right)$$

$$\cong 1 - e^{-\frac{1}{n}} \times e^{-\frac{2}{n}} \times \ldots \times e^{-\frac{k-1}{n}}$$

$$= 1 - e^{-\frac{k(k-1)}{2n}}$$

To find k such that $P(n,k) \geq 0.5$ we have

$$\frac{1}{2} \leq 1 - e^{-\frac{k(k-1)}{2n}}$$

$$2 \leq e^{\frac{k(k-1)}{2n}}$$

$$\ln 2 \leq \frac{k(k-1)}{2n}$$

$$k^2 - k - 2n \ln 2 \geq 0$$

$$k_{1,2} = \frac{1 \pm \sqrt{1 + 8n \ln n}}{2}$$

We are only interested in the $k \geq k_1$, as we can not have negative number of people.

$$k_1 \approx \frac{\sqrt{8n \ln n}}{2} = \sqrt{2n \ln n} \approx 1.18\sqrt{n}$$

For n=365, we have $k_1 \approx 22.54$

Therefore, we need at least 23 people in order for the probability that at least 2 people share a birthday to be at least 0.5.

For analysis of Birthday attack, see text Appendix 11A.

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

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

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

Signature = (r, s)

Verifying

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

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

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

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

TEST: $v = r'$

M = message to be signed

$H(M)$ = hash of M using SHA-1

M', r', s' = received versions of M, r, s

Figure 13.4 The Digital Signature Algorithm (DSA)

Solution (text): We first show the following.

If $g = h^{\frac{p-1}{q}} \bmod p$ then $g^t \bmod p = g^{t \bmod q} \bmod p$, for any integer t. (1)

For any integer $t = nq + z$, where n and z are non-negative integers we have

$$\begin{aligned} g^t mod\ p &= g^{nq+z} \bmod p \\ &= (g^{nq} \bmod p)(g^z \bmod p) \bmod p \\ &= (h^{\frac{p-1}{q}} \bmod p)^{nq} (g^z \bmod p) \bmod p \\ &= \left(h^{(p-1)n} \bmod p\right)(g^z \bmod p) \bmod p \\ &= \left(h^{(p-1)} \bmod p\right)^n (g^z \bmod p) \bmod p \qquad \textbf{by Fermat's Little Theorem} \\ &= 1^n g^z \bmod p = g^z \bmod p = g^{t \bmod q} \bmod p \end{aligned}$$

We then show the following:

$g^{a \bmod q + b \bmod q} \bmod p = g^{(a+b) \bmod q} \bmod p$ (2)

Indeed, we have

$$g^{a \bmod q + b \bmod q} \bmod p = g^{(a \bmod q + b \bmod q) \bmod q} \bmod p \qquad \textbf{by (1)}$$
$$= g^{(a+b) \bmod q} \bmod p$$

We now show that $v = r$ if the signature is valid.

$$v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$$

$$= ((g^{(H(M)w) \bmod q} y^{(rw) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(H(M)w) \bmod q} (g^x \bmod p)^{(rw) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(H(M)w) \bmod q} g^{(x((rw) \bmod q) \bmod q}) \bmod p) \bmod q \qquad \textbf{by (1)}$$

$$= ((g^{(H(M)w) \bmod q + (xrw) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(H(M)w + xrw) \bmod q}) \bmod p) \bmod q \qquad \textbf{by (2)}$$

$$= ((g^{((H(M)+xr)w) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(((H(M)+xr) \bmod q)\,(w \bmod q)) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(((sk) \bmod q)\,(w \bmod q)) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(skw) \bmod q}) \bmod p) \bmod q$$

$$= ((g^{(((k) \bmod q)\,(ws \bmod q)) \bmod q}) \bmod p) \bmod q$$

$$= (g^{k \bmod q} \bmod p) \bmod q$$

$$= (g^k \bmod p) \bmod q \qquad \textbf{by (1)}$$
$$= r$$