CAB340 – ASSESSMENT 3

Public-key encryption, Secret Sharing

Callum McNeilage – n10482652 Folder: 152-Student

1 Number Theory

a)

i)

$$a \equiv b (\bmod\, n)$$
$$p^{-1}p \equiv 1 (\bmod\, q)$$
$$\therefore a - b = \ell n \equiv (p^{-1}p) - 1 = \ell q, k \in \mathbb{Z}$$

ii)

If there exists integers m, n such that $pm + qn = 1$, then there exists $pm = (-n)q + 1$ and therefore $pm = 1 (\bmod\, q)$ where $m = p^{-1}$

b)

j	a_j	b_j	q_j	r_j	$a_j = b_j \times q_j + r_j$
0	29	17	$\frac{29}{17} = 1r12$	12	$29 = 17 \times 1 + 12$
1	$b_{j-1} = 17$	$r_{j-1} = 12$	$\frac{17}{12} = 1r5$	5	$17 = 12 \times 1 + 5$
2	12	5	$\frac{12}{5} = 2r2$	2	$12 = 5 \times 2 + 2$
3	5	2	$\frac{5}{2} = 2r1$	1	$5 = 2 \times 2 + 1$
4	2	1	$\frac{2}{1} = 2r0$	0	$2 = 1 \times 2 + 0$

$$gcd(29,17) = gcd(2,1) = 1$$

c)

j	a_j	b_j	q_j	m_j	n_j	$a_j \times m_j + b_j \times n_j = gcd(a, b)$
3	5	2	$\frac{5}{2} = 2$	1	-2	$5 \times 1 + 2 \times -2 = 1$
2	12	5	$\frac{12}{5} = 2$	-2	5	$12 \times -2 + 5 \times 5 = 1$
1	17	12	$\frac{17}{12} = 1$	5	-7	$17 \times 5 + 12 \times -7 = 1$
0	29	17	$\frac{29}{17} = 1$	-7	12	$29 \times -7 + 17 \times 12 = 1$

d)

$$am + bn = gcd(a, b)$$
$$29 \times -7 + 17 \times 12 = gcd(29,17) = 1$$
$$x = 12, y = 10$$

2 RSA Encryption

a)

$$\begin{aligned}
p &= 2027\\
q &= 2593\\
e &= 17\\
n &= p \times q = 2027 \times 2593 = 5256011\\
\phi(n) &= (p-1)(q-1) = (2027-1)(2593-1) = (2026)(2592) = 5251392\\
d &= e^{-1} \bmod \phi(n) = 17^{-1} \bmod 5251392 = 3706865
\end{aligned}$$

i)

Public Key = $\phi(n) = 5251392$

ii)

Private Key = $d = 3706865$

b)

$$\begin{aligned}
C &= M^{e} \bmod n\\
C &= 1024^{17} \bmod 5256011\\
C &= 4104975
\end{aligned}$$

c)

$$\begin{aligned}
M &= C^{d} \bmod n\\
M &= 775360^{3706165} \bmod 5256011\\
M &= 11111
\end{aligned}$$

d)

$$\left.\begin{aligned} p &= 2711\\ q &= 2713 \end{aligned}\right\} \text{Found using Wolfram Alpha}$$

$$\begin{aligned}
n &= 7354943\\
e &= 7\\
\phi(n) &= (p-1)(q-1) = (2711-1)(2713-1) = (2710)(2712) = 7349520\\
d &= e^{-1} \bmod \phi(n) = 7^{-1} \bmod 7349520 = 2099863
\end{aligned}$$

Private Key = 2099863

3 Digital Signatures

a)

Because the server requires signing the bare challenge without hashing, the server can easily distinguish the challenge body and Alice's digital signature. Therefore, if the server sends a hashed email as its randomly chosen number, it can forge emails from Alice.

b)

The suggested modification to the server authentication protocol is to hash the challenge. This will defeat the attack above as in order for the server to complete the attack it must find a collision (x,y) such that h(x) = h(y).

4 Diffie-Hellman Key Agreement

4.1 A (too) simple implementation

a)

x	Order of x modulo 2027
1	$1^{1013}\%2027 = 1$
2	$2^{1013}\%2027 = 2026$
3	$3^{1013}\%2027 = 1$
4	$4^{1013}\%2027 = 1$
5	$5^{1013}\%2027 = 2026$
6	$6^{1013}\%2027 = 2026$
7	$7^{1013}\%2027 = 2026$
8	$8^{1013}\%2027 = 2026$
9	$9^{1013}\%2027 = 1$
10	$10^{1013}\%2027 = 1$

2,5,6,7,8 are generators

b)
Using bc:

$$6^{1013} \bmod 2027 = 2026$$
$$3^{1013} \bmod 2027 = 1$$

c)

$$p = 2027$$
$$g = 2$$
$$a = 123$$
$$b = 456$$
$$A = g^{\mathrm{a}} \bmod 2027$$
$$A = 2^{123} \bmod 2027$$
$$A = 1561$$
$$B = g^{\mathrm{b}} \bmod 2027$$
$$B = 2^{456} \bmod 2027$$
$$B = 211$$

A = 1561, B = 211

d)

$$s = B^{a} \bmod p$$
$$s = 211^{123} \bmod 2027$$
$$s = 238$$

$$s' = A^{b} \bmod p$$
$$s' = 1561^{456} \bmod 2027$$
$$s' = 238$$

4.2 An attack and a fix

a)

$$\begin{aligned}&A = 1561\\&B = 211\\&A_2 = A^{1013} \bmod 2027\\&A_2 = 1561^{1013} \bmod 2027\\&A_2 = 2026\\&B_2 = B^{1013} \bmod 2027\\&B_2 = 211^{1013} \bmod 2027\\&B_2 = 1\end{aligned}$$

Residues are $A_2 = 2026$, $B_2 = 1$

b)

$$\begin{aligned}&g = 2\\&g_2 = 2^{1013} \bmod 2027\\&g_2 = 2026\end{aligned}$$

Yes, the residue of the generator is always 2026 for this problem.

c)

$$\begin{aligned}&A = g^a \bmod 2027\\&1561 = 2^a \bmod 2027\\&a = 123\\&B = \mathrm{g}^b \bmod 2027\\&211 = 2^a \bmod 2027\\&b = 456\end{aligned}$$

d)

$$\begin{aligned}&S = 2^{456\cdot 123} \bmod 2027\\&S = 238\\&S' = 2^{123\cdot 456} \bmod 2027\\&S' = 238\end{aligned}$$

Therefore, residue $K_2 = 238$

Verify:

$$\begin{aligned}&K^{1013} \bmod 2027 = 1\\&238^{1013} \bmod 2027 = 1\\&1 = 1\end{aligned}$$

5 Secret Sharing

a)
If party m XORs there string from party j with every value r_j they can reconstruct the secret x

b)
To retrieve the secret x, all information is required. For instance, in a 1 byte secret, with each party receiving 1 bit of information, if one party does not provide their bit of information, the secret can have 2 possible values and it is impossible to derive which is correct.

c)
for $u_1 = s_1 \oplus t_1$

$u_2 = s_2 \oplus t_2$

$u_3 = s_1 \oplus t_1 \ \oplus x \oplus s_2 \oplus t_2 \oplus y$

$$u_1 \oplus u_2 \oplus u_3 = x \oplus y$$