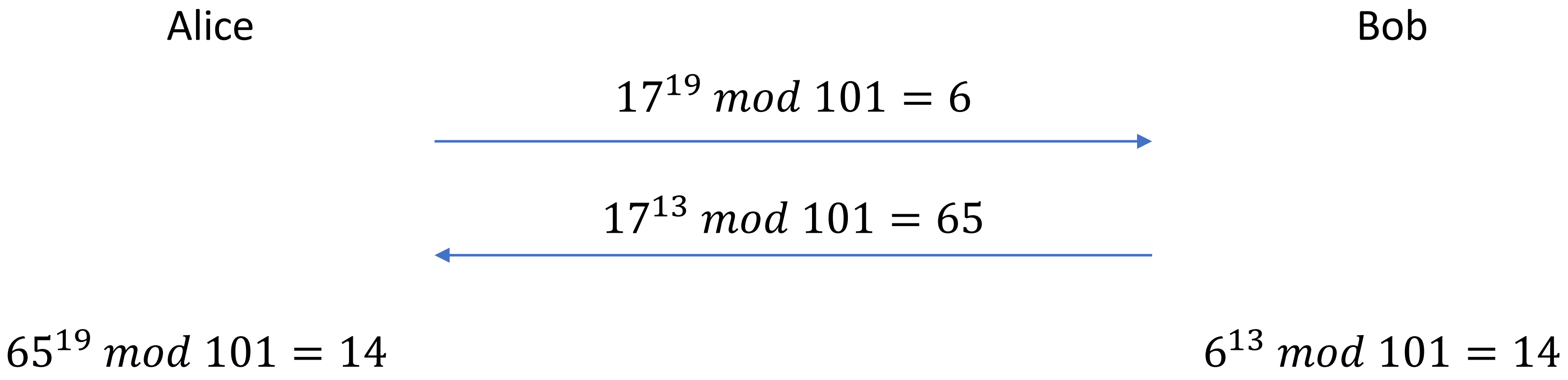
Tutorial -4

SOEN-321

Problem 1

Suppose that users Alice and Bob carry out the Diffie-Hellman key agreement protocol with p = 101 and g = 17. Suppose that Alice chooses x = 19 and Bob chooses y = 13. Show the computations performed by both Alice and Bob and determine the key that they will share.



Alice

Bob

$17^{19}\ mod\ 101 = 6$

$17^{13}\ mod\ 101 = 65$

$65^{19}\ mod\ 101 = 14$

$6^{13}\ mod\ 101 = 14$

$17^{19}\ mod\ 101$

$19 = 10011$

$17^{1} = 17\ mod\ 101 = 17$

$17^{2} = 17^{2}\ mod\ 101 = 87$

$17^{4} = 87^{2}\ mod\ 101 = 95$

$17^{8} = 95^{2}\ mod\ 101 = 36$

$17^{16} = 36^{2}\ mod\ 101 = 84$

$17^{19} = 17 \times 87 \times 84\ mod\ 101 = 6$

$6^{13}\ mod\ 101$

$13 = 1101$

$6^{1} = 6\ mod\ 101 = 6$

$6^{2} = 6^{2}\ mod\ 101 = 36$

$6^{4} = 36^{2}\ mod\ 101 = 84$

$6^{8} = 84^{2}\ mod\ 101 = 87$

$6^{13} = 6 \times 84 \times 87\ mod\ 101 = 14$

$17^{13}\ mod\ 101$

$13 = 1101$

$17^{1} = 17\ mod\ 101 = 17$

$17^{2} = 17^{2}\ mod\ 101 = 87$

$17^{4} = 87^{2}\ mod\ 101 = 95$

$17^{8} = 95^{2}\ mod\ 101 = 36$

$17^{13} = 17 \times 95 \times 36\ mod\ 101 = 65$

$65^{19}\ mod\ 101$

$19 = 10011$

$65^{1} = 65\ mod\ 101 = 65$

$65^{2} = 65^{2}\ mod\ 101 = 84$

$65^{4} = 84^{2}\ mod\ 101 = 87$

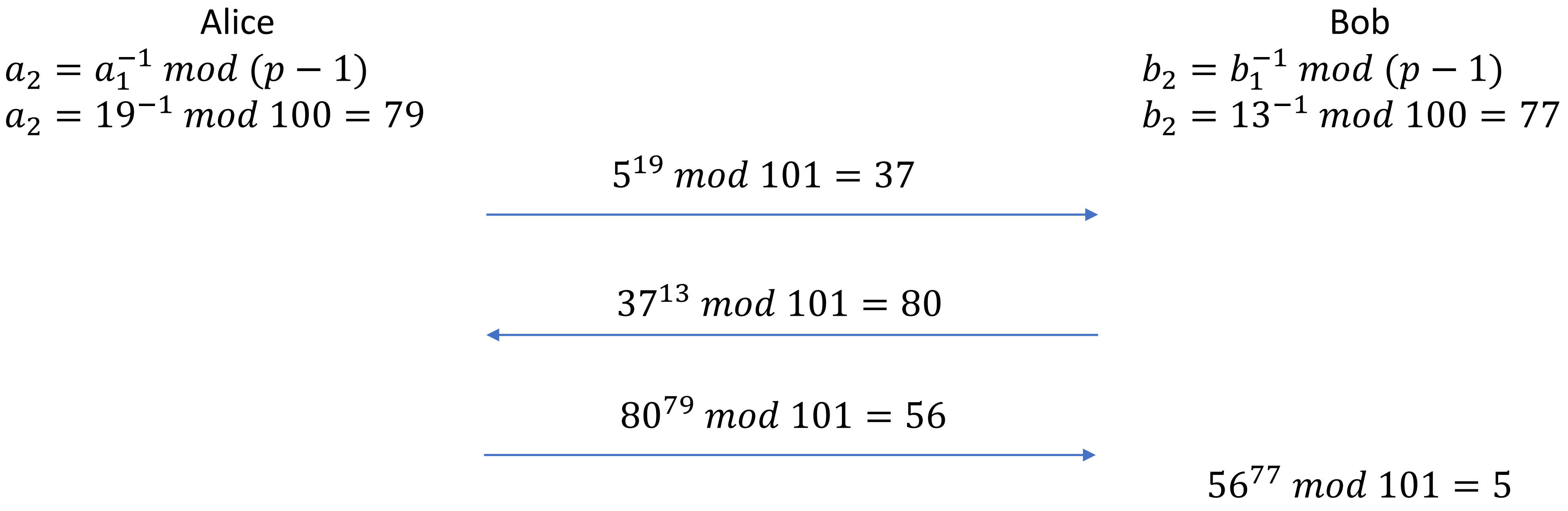
$65^{8} = 87^{2}\ mod\ 101 = 95$

$65^{16} = 95^{2}\ mod\ 101 = 36$

$65^{19} = 65 \times 84 \times 36\ mod\ 101 = 14$

Problem 2

Suppose that users Alice and Bob carry out the 3-pass Diffie-Hellman protocol with p = 101. Suppose that Alice chooses a1= 19 and Bob chooses b1= 13. If Alice wants to send the secret message m =5 to Bob, show all the messages exchanged between Alice and Bob



Alice

$$a_2 = a_1^{-1}\, mod\ (p-1)$$
$$a_2 = 19^{-1}\, mod\ 100 = 79$$

Bob

$$b_2 = b_1^{-1}\, mod\ (p-1)$$
$$b_2 = 13^{-1}\, mod\ 100 = 77$$

$$5^{19}\, mod\ 101 = 37$$

$$37^{13}\, mod\ 101 = 80$$

$$80^{79}\, mod\ 101 = 56$$

$$56^{77}\, mod\ 101 = 5$$

$$\begin{array}{l}
19^{-1}\ mod\ 100 \\
100 = 5 \times 19 + 5 \\
19\ \ = 3 \times 5 + 4 \\
5 = 1 \times 4 + 1 \\
1 = 5 - 4 \\
1 = 5 - (19 - 3 \times 5) \\
1 = 4 \times 5 - 19 \\
1 = 4(100\ \ - 5 \times 19) - 19 \\
1 = 4 \times 100\ \ - 21 \times 19 \\
1 = 79 \times 19\ mod\ 100
\end{array}$$

$$\begin{array}{l}
13^{-1}\ mod\ 100 \\
100 = 7 \times 13 + 9 \\
13\ \ = 1 \times 9 + 4 \\
9 = 2 \times 4 + 1 \\
1 = 9 - 2 \times 4 \\
1 = 9 - 2(13 - 9) \\
1 = 3 \times 9 - 2 \times 13 \\
1 = 3(100\ \ - 7 \times 13) - 2 \times 19 \\
1 = 3 \times 100\ \ - 23 \times 13 \\
1 = 77 \times 19\ mod\ 100
\end{array}$$

$$\begin{array}{l}
80^{79}\ mod\ 101 \\
79 = 1001111 \\
80\ \ = 80 mod\ 101 = 80 \\
80^{2}\ \ = 80^{2}\ mod\ 101 = 37 \\
80^{4}\ \ = 37^{2}\ mod\ 101 = 56 \\
80^{8}\ \ = 56^{2}\ mod\ 101 = 5 \\
80^{16}\ = 5^{2}\ mod\ 101 = 25 \\
80^{32}\ = 25^{2}\ mod\ 101 = 19 \\
80^{64}\ = 19^{2}\ mod\ 101 = 58 \\
80^{79}\ = 80 \times 37 \times 56 \times 5 \times 58\ mod\ 101 = 56
\end{array}$$

$$\begin{array}{l}
5^{19}\ mod\ 101 \\
19 = 10011 \\
5^{1}\ \ = 5\ mod\ 101 = 5 \\
5^{2}\ \ = 5^{2}\ mod\ 101 = 25 \\
5^{4}\ \ = 25^{2}\ mod\ 101 = 19 \\
5^{8}\ \ = 19^{2}\ mod\ 101 = 58 \\
5^{16}\ = 58^{2}\ mod\ 101 = 31 \\
5^{19}\ = 5 \times 25 \times 31\ mod\ 101 = 37
\end{array}$$

$$\begin{array}{l}
37^{13}\ mod\ 101 \\
13 = 1101 \\
37^{1}\ \ = 37\ mod\ 101 =37 \\
37^{2}\ \ = 37^{2}\ mod\ 101 = 56 \\
37\ \ = 56^{2}\ mod\ 101 =5 \\
37^{8}\ \ = 5^{2}\ mod\ 101 = 25 \\
5^{19}\ = 37 \times 5 \times 25\ mod\ 101 = 80
\end{array}$$

$$\begin{array}{l}
56^{77}\ mod\ 101 \\
77 = 1001101 \\
56\ \ = 56\ mod\ 101 = 56 \\
56^{2}\ \ = 56^{2}\ mod\ 101 = 5 \\
56^{4}\ \ = 5^{2}\ mod\ 101 = 25 \\
56^{8}\ \ = 25^{2}\ mod\ 101 = 19 \\
56^{16}\ = 19^{2}\ mod\ 101 = 58 \\
56^{32}\ = 58^{2}\ mod\ 101 = 31 \\
56^{64}\ = 31^{2}\ mod\ 101 = 52 \\
56^{79}\ = 56 \times 25 \times 19 \times 52\ mod\ 101 = 5
\end{array}$$

Problem 3

Consider an RSA system where the public key of three users (i.e., (n,e) are given by: (319,3), (697,3) and (1081,3). If the same message was sent to the three users. Show how the attacker can recover m by observing the ciphertexts c1=128, c2=34 and c3=589.

$m^e = c \; mod \; n$

let's refer to m^e as x, then we can have the following equations

$$x = 128 \; mod \; 319$$
$$x = 34 \quad mod \; 697$$
$$x = 589 \; mod \; 1081$$

$m_1 = 697 \times 1081 = 753457$

$y_1 = 753457^{-1} \; mod \; 319$

$y_1 = 298^{-1} \; mod \; 319 = 243$

$m_2 = 319 \times 1081 = 344839$

$y_2 = 344839^{-1} \; mod \; 697$

$y_2 = 521^{-1} \; mod \; 697 = 99$

$m_3 = 319 \times 697 = 222343$

$y_3 = 222343^{-1} \; mod \; 1081$

$y_3 = 738^{-1} \; mod \; 1081 = 104$

$x = \sum a_i m_i y_i \;\; mod \; N$

$N = 319 \times 697 \times 1081 = 240352783$

$x = (128 \times 753457 \times 243 + 34 \times 344839 \times 99 + 589 \times 222343 \times 104) \; mod \; 240352783 = 4913$

$m = \sqrt[3]{x} = \sqrt[3]{4913} = 17$

$298^{-1}\ mod\ 319$

$319 = 1 \times 298 + 21$

$298 = 14 \times 21 + 4$

$21 = 5 \times 4 + 1$

$1 = 21 - 5 \times 4$

$1 = 21 - 5(298 - 14 \times 21)$

$1 = 71 \times 21 - 5 \times 298$

$1 = 71(319 - 298) - 5 \times 298$

$1 = 71 \times 319 - 76 \times 298$

$1 = 243 \times 298\ mod\ 319$

$521^{-1}\ mod\ 697$

$697 = 1 \times 521 + 176$

$521 = 2 \times 176 + 169$

$176 = 1 \times 169 + 7$

$169 = 24 \times 7 + 1$

$1 = 169 - 24 \times 7$

$1 = 169 - 24(176 - 169)$

$1 = 25 \times 169 - 24 \times 176$

$1 = 25(521 - 2 \times 176) - 24 \times 176$

$1 = 25 \times 521 - 74 \times 176$

$1 = 25 \times 521 - 74(697 - 521)$

$1 = 99 \times 521 - 74 \times 697$

$1 = 99 \times 521\ mod\ 697$

$738^{-1}\ mod\ 1081$

$1081 = 1 \times 738 + 343$

$738 = 2 \times 343 + 52$

$343 = 6 \times 52 + 31$

$52 = 1 \times 31 + 21$

$31 = 1 \times 21 + 10$

$21 = 2 \times 10 + 1$

$1 = 21 - 2 \times 10$

$1 = 21 - 2(31 - 21)$

$1 = 3 \times 21 - 2 \times 31$

$1 = 3(52 - 31) - 2 \times 31$

$1 = 3 \times 52 - 5 \times 31$

$1 = 3 \times 52 - 5(343 - 6 \times 52)$

$1 = 33 \times 52 - 5 \times 343$

$1 = 33(738 - 2 \times 343) - 5 \times 343$

$1 = 33 \times 738 - 71 \times 343$

$1 = 33 \times 738 - 71(1081 - 738)$

$1 = 104 \times 738 - 71 \times 1081$

$1 = 104 \times 738\ mod\ 1081$