Alexandra (Anna) Burke
COSC 4343

Homework #3

Question #1

Part 1:

Alice public key $(N,e) = (21,5)$

- choose p and q so $p \neq q$

$p=3, q=17$

- Compute ϕN

$(3-1)(17-1) = 32$

- Choose e relatively prime to ϕN

$e=3$

- Find d, such that $(e)(d) \% \phi N = 1$

$3(d) \bmod 32 = 1$

$d = 11$

public key $(N,e) = (32,3)$

private key $(N,e) = (32,11)$

Part 2:

plain text = "Anna Burke"

ASCII = 34, 97, 110, 110, 97, 32, 98, 117, 114, 107, 101, 34

Encryption: $C = m^e \bmod N$

$(N,e) = (21,5)$

DIGIT	C		$C = m^e \bmod N$
0	0	=	$0^5 \bmod 21$
1	1	=	$1^5 \bmod 21$
2	11	=	$2^5 \bmod 21$
3	12	=	$3^5 \bmod 21$
4	16	=	$4^5 \bmod 21$
5	17	=	$5^5 \bmod 21$
6	6	=	$6^5 \bmod 21$
7	7	=	$7^5 \bmod 21$
8	8	=	$8^5 \bmod 21$
9	18	=	$9^5 \bmod 21$

encrypted message: 1216, 187, 110, 110, 187, 1211, 188, 117, 1116, 107, 101, 1216

Part 3:

plain text = "Anna Burke"

ASCII = 34, 97, 110, 110, 97, 32, 98, 117, 119, 107, 101, 34

Sign formula: $S = m^d \bmod N$

(N,d) Senders private key: (32, 11)

DIGIT	S		
0	0	=	$0^{11} \bmod 32$
1	11	=	$1^{11} \bmod 32$
2	25	=	$2^{11} \bmod 32$
3	19	=	$3^{11} \bmod 32$
4	17	=	$4^{11} \bmod 32$
5	27	=	$5^{11} \bmod 32$
6	9	=	$6^{11} \bmod 32$
7	3	=	$7^{11} \bmod 32$
8	1	=	$8^{11} \bmod 32$
9	11	=	$9^{11} \bmod 32$

Signed Message = 1917, 113, 110, 110, 113, 1925, 111, 113, 1117, 103, 101, 1917

Part 4:

Encrypted Message: 1216, 187, 110, 110, 187, 1211, 188, 117, 1116, 107, 101, 1216

Senders Private Key = (32, 11)

DIGIT	S		
0	0	=	$0^{11} \bmod 32$
1	11	=	$1^{11} \bmod 32$
2	25	=	$2^{11} \bmod 32$
3	19	=	$3^{11} \bmod 32$
4	17	=	$4^{11} \bmod 32$
5	27	=	$5^{11} \bmod 32$
6	9	=	$6^{11} \bmod 32$
7	3	=	$7^{11} \bmod 32$
8	1	=	$8^{11} \bmod 32$
9	11	=	$9^{11} \bmod 32$

$[\{M\}] =$ 1917, 113, 110, 110, 113, 1925, 111, 113, 1117, 103, 101, 1917

Part 5:

Signed Message: 1917, 113, 110, 110, 113, 1925, 111, 113, 1117, 103, 101, 1917

Recievers Public Key = (21, 5)

DIGIT	C		$C = m^e \bmod N$
0	0	=	$0^5 \bmod 21$
1	1	=	$1^5 \bmod 21$
2	11	=	$2^5 \bmod 21$
3	12	=	$3^5 \bmod 21$
4	16	=	$4^5 \bmod 21$
5	17	=	$5^5 \bmod 21$
6	6	=	$6^5 \bmod 21$
7	7	=	$7^5 \bmod 21$
8	8	=	$8^5 \bmod 21$
9	18	=	$9^5 \bmod 21$

$\{[M]\} =$ 11817, 1112, 110, 110, 1112, 118117, 111, 1112, 1117, 1012, 101, 11817

Question #2

$p = 541$

$g = 10$

Alice: $A = 11$

Bob: $B = 13$

Alice → Bob: $g^a \bmod p$

$10^{11} \bmod 541 = 297$

Bob → Alice: $g^b \bmod p$

$10^{13} \bmod 541 = 486$

Bob computes:

$297^{13} \bmod 541 = 511$

$(g^a \bmod p)^b \bmod p$

Alice Computes:

$486^{11} \bmod 541 = 511$

$(g^b \bmod p)^a \bmod p$

Symmetric Key