

# MATH 30A

## RSA PUBLIC KEY CRYPTOGRAPHY

### Key formulas with examples:

1)  $n = pq$ , where  $p$  and  $q$  are prime numbers

Example:  $n = 22$ ,  $p = 2$ ,  $q = 11$

2)  $k \equiv 1 \pmod{(p-1)(q-1)}$ , where  $k$  is composite

Example: With  $p = 2$ ,  $q = 11$ ,  $k \equiv 1 \pmod{(2-1)(11-1)} \equiv 1 \pmod{10}$ . That is, possible values for  $k$  are  $k = 1, 11, 21, 31$ , etc. The smallest composite number that works is  $k = 21$ .

3) Factor  $k = e \cdot d$

Example:  $21 = 7 \cdot 3$ , so  $e = 7$  and  $d = 3$ , or vice versa.  $e$  will be used to encode and is made public, along with  $n$ .  $d$  will be used to decode and is kept secret.

4) Calculate  $C \equiv W^e \pmod{n}$  to encode the message  $W$  (a number between 1 and  $n-1$ ).  $C$  will be the encoded message.

Example: To encode the message  $W = 13$ ,  $C \equiv 13^7 \pmod{22} \equiv 7 \pmod{22}$ , so the encoded message is  $C = 7$ .

5) Calculate  $W \equiv C^d \pmod{n}$  to decode the message  $C$ . The decoded message is  $W$ .

Example: To decode the message  $C = 7$ ,  $W \equiv 7^3 \pmod{22} \equiv 13 \pmod{22}$ , so the decoded message is  $W = 13$ .

**Group activity:** Your group will be assigned one of the following 6 codes:

Code 1  $n = 55$   $e = 23$   $d =$

Code 2  $n = 65$   $e = 29$   $d =$

Code 3  $n = 85$   $e = 13$   $d =$

Code 4  $n = 77$   $e = 37$   $d =$

Code 5  $n = 91$   $e = 29$   $d =$

Code 6  $n = 95$   $e = 31$   $d =$

1) In your group, create a two-letter message.

2) Encode the two letters using the code for the group to which you're sending it and give the encoded message to that group.

3) When you receive the message from the other group, decode it using the code for your group.

4) When you're done, figure out the value of  $d$  for the other group's code.

### Numerical codes for letters of the alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26