CAESAR CIPHER

Practice: Encode or decode the following words:

Shift=

Plain	H	E	L	L	O
Ciphered					

Shift=

Plain				
Ciphered	T	H	-	O

Group activity: Your mission is to send a message, encoded using Caesar cipher, to the other team, without the enemies of the Jedi being able to read it.

Secret shift: Only members of your team and the receiver team can know it!

Encode your message

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Plain															
Ciphered															

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Plain															
Ciphered															

Decode your allies' message

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ciphered															
Plain															

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Ciphered															
Plain															

Activity: Try to decode my message without knowing the shift.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C																									

MODULAR ARITHMETIC

Practice: Compute the following modular reductions:

Use WolframAlpha!

www.wolframalpha.com

$17 \pmod 5 =$

$138 \pmod{14} =$

$17294803 \pmod{269} =$

Practice: Compute the following modular operations:

$5 + 6 \pmod 7 =$

$5 \times 6 \pmod 7 =$

$5^6 \pmod 7 =$

$38 + 52 \pmod 3 =$

$38 \times 52 \pmod 3 =$

$38^{52} \pmod 3 =$

$1329 + 2963 \pmod 6 =$

$1329 \times 2963 \pmod 6 =$

$1329^{2963} \pmod 6 =$

Practice: Write the multiplication table modulo 6:

$\times$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

RSA CRYPTOSYSTEM

KEY GENERATION

1. Choose two large prime numbers p and q from the list:

   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293

   They are secret: only people in your team can know them!

2. Compute $n = p \times q$.
3. Compute $\phi = (p-1) \times (q-1)$.
4. Choose a prime number e smaller than ϕ such that $\gcd(e, \phi) = 1$ (check with WolframAlpha).
5. Find the inverse of e modulo ϕ. Call it $d = e^{-1} \pmod{\phi}$. Also secret!

Public key: (n, e). Give it to anyone who wants to send you a message!
Private key: d. Super secret! Only you (and your team) should know it.

ENCODING

You are now the sender of the message.

1. Convert each letter of your message into a number m. Use this table:

	A	B	C	D	E	F	G	H	I	J	K	L	M
0	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

2. Using the receiver's public key (n, e), compute $c = m^e \pmod{n}$.

The encoded message is c. You can send it to the receiver now.

DECODING

You are now the receiver of the message.

1. Using your public and private keys (n, e) and d, compute $m = c^d \pmod{n}$.

   This is the decoded message!

2. Convert the numerical message into a letter again, using the same table as before. You recover the letter that was sent to you.

RSA PRACTICE

Group activity: Reinforcements have arrived, but the enemies have managed to break your previous Caesar cipher. Then, the only way you can communicate with your allies is using RSA encryption, that does not require both teams to know the same key. Your mission is to send a message, using RSA cryptosystem, to the other team. Then, you decode the message you have received.

GENERATE YOUR KEY

1. Choose your prime numbers (with your team). Super secret!!

   $p =$ $q =$

2. $n =$ 3. $\phi =$

4. Choose (with your team) the prime number $e =$

5. Super secret!! $d =$

Your public key **Private key (Secret)**

$(n, e) =$ (,) $d =$

ENCODE YOUR MESSAGE

Receiver's public key: $(n, e) =$ (,)

	1	2	3	4	5	6	7	8	9	10
Plain										
Numbers										
Ciphered										

	11	12	13	14	15	16	17	18	19	20
Plain										
Numbers										
Ciphered										

DECODE YOUR ALLIES' MESSAGE

Your public key **Private key (Secret)**

$(n, e) =$ (,) $d =$

	1	2	3	4	5	6	7	8	9	10
Ciphered										
Numbers										
Plain										

	11	12	13	14	15	16	17	18	19	20
Ciphered										
Numbers										
Plain										