Caesar Cipher

We intercept the following cipher text (encoded message):

F QEFKH TB KBBA X YBQQBO ZLAB. QEBV YOLHB QEFP LKB OBXIIV CXPQ.

Our intelligence agency thinks it is a Caesar cipher, but they don't know the shift.

The spaces are preserved in this message, so we can use that information to figure out the shift, but it may take some trial and error. We don't want to try all 26 options, try to narrow it down.

Write the plain text (decoded message) below:

Caesar Cipher

Use the following tables to help decode the message. For example, if we thought the shift was 7, our table would become:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

And we would decode our message by looking at the letter under the letter in the cipher text.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher

It seems our adversaries are getting smarter. We intercept the following cipher text:

OLEUANGBKGRUTMSKYYGMKLXKWAKTIEZGHRKYHKIUSKBKXEAYKLAR.JUEUAGMXKK?

It seems they were smart enough to remove all the spaces between words. What else can we use to figure out the shift?

Hint: Would it be more common to see "Q" or "A" in the original message? What is the most common letter in English?

Write the plain text (decoded message) below:

Once you have decoded this message, think about the following questions:

1. Is it better to intercept a long message or a short message? Why?
2. Would our method of breaking this code work in Spain?
3. How could you improve this code?

Block Cipher

Let's say we want to encode the message:

I LIKE HOTDOGS

We write our message in a block form. We have 12 letters, so we may choose a 3x4 block.

I L I K

EHOT

DOGS

We write the letters down each column to get the cipher text:

IEDLHOIOGKTS

When we intercept a cipher text, but we do not know the size of the block. Try to determine the block size and decode the following cipher text:

WSLEIEDZOOEFNSTOTWTOOWBP AERNSITOMOMEUENRMUBUMLLBOTECIRKPS

If you are stuck, think about how you would decode the first message if you knew what the block size (in that case the block size was 3x4).

Once you have decoded the cipher text, answer the following questions:

1. What happens if the block is not completely filled?
2. Can you think of ways to use something a key other than a block? (Hint: Sudoku and a marker)
3. Is it better to intercept a longer or shorter cipher text? Why?

Coin Flip Over the Phone

You are on the phone with your friend, when NASA calls and puts both of you on the phone. They say they have one more seat on the next shuttle mission, and it has come down to the two of you. NASA is unable to make the final choice, so they leave it up to you and your friend to decide who gets to go to Mars. They need an answer in the next 5 minutes, and your friend lives 20 minutes away, so you will need to make a decision over the phone.

Can you think of a method you both agree to, which gives a 50% chance of winning for each person?

Is there any way for either person to cheat using your method?

Coin Flip Over the Phone

Use the following steps to "flip a coin" over the phone with your partner. Decide now who is Player A and who is Player B.

Player A:

1. Pick two prime numbers (don't tell anyone what you choose, but remember them).
2. Multiply the two prime numbers you choose together.
3. Tell Player B the product you just computed (do NOT tell them the original two primes).

Person B:

1. Once Player A tells you the number they computed, make a guess "Heads" or "Tails" and tell it to Player A.

You should now work together to see who won the "coin flip".

1. Player A reveals the two original prime numbers.
2. Both players should check that they multiple to the right number (i.e. the number Player A told Player B before he/she guessed "Heads" or "Tails").
3. Add up the digits of the two original prime numbers.
   If the sum is even then the correct guess for Player B to win was "Heads"
   If the sum is odd then the correct guess for Player B to win was "Tails"
   If Player B guessed wrong, then Player A won.

Questions about our game:

1. Does the game give a 50% chance to each player?
2. If you could choose, would you want to be Player A or Player B?
3. Is it possible to cheat at this game?

HEADS

TAILS

Pigpen Cipher

We can use shapes to encrypt information. Say we want to encode the message:

“Rats are the best pets.”

Using the key

Then our encoded message becomes:

Pigpen Cipher

Try to decode the following cipher text. Remember that we do not necessarily know the shape of the key. Some trial and error may be necessary.

After you decode the cipher text answer the following questions:

1. Can you come up with a different key shape to use? Would your new system be harder or easier for someone to break than the system above?
2. How could you improve the key for the pigpen cipher used above?
3. Would you prefer to intercept a longer or shorter cipher text? Why?

Code Mastery

You now have the skills to crack multiple codes. In the real world, you may not know which system your adversaries used to encode their messages. The following codes use some variation of methods we have learned today. See how many you can crack!

Cipher Text 1:

IOEHNIAYSVAGENRADEPHY

Cipher Text 2:

Cipher Text 3:

SDAJYNULPKHKCUEOKQPHWSAZ KJHUPDAKQPHWSOSEHHXAOAYQNA

Cipher Text 4:

JXQDAOEKVEHSECYDW JECQJXSYHSBUYXQTQBEJEVVKDJUQSXYDWOEKSETUI

List of Primes

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	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		