# Encryption/Decryption Activity

We’re going to do an activity to try and help you understand symmetric and asymmetric encryption. You’ll want to do this with a text file where you record the various secrets you uncover – that’s what you’ll submit at the end of the activity.

## Step 1: Symmetric Encryption

So symmetric encryption is basically just using math to encode some data into what we’ll call ciphertext. Here’s an example of some ciphertext:

y1NiB4qtUNDR5OEzZGT1kOwtnxfkbltEw/pKYBgmVtQ=

This ciphertext doesn’t mean anything to you without an important detail – the secret password or key is cDQxPM79dTtYsUgb

Now that you know that, you should be able to go to this website <https://www.devglan.com/online-tools/aes-encryption-decryption> and enter in the text and the key (everything else left to defaults is fine). You should be able to recover my message – put the secret word in the file you’re turning in for homework. NOTE: You’ll have to decrypt, and then you’ll have to press the “decode to plain text” at the bottom for it to work.

Woo hoo! Let’s not get into the heavy math that makes this encoding work. Let’s just point out one key detail – the key that you used to decrypt the message is the same key I used to encrypt the message. That’s what makes the encryption symmetric. So now that you know my secret key, you can encrypt messages using it just like I can.

## Step 2a: Asymmetric Encryption - Signing

So we start out the same way. Here’s some ciphertext:

ft1bdv08I++uvYjbWX8i0kMMzP1mADl1n9pkICncNOISQq/FeQGNcErMM6dHFzswfegRiDsFN4drS9lnLUb7tIzPDHDOQb95R96C4fXrRTpxA3Lwj7p/ZK38apyP4e2Jr0VpsMZPtsmOY5CrZo9nN4KQ2IAdFU+n9KgwlLTVrA0=

Here’s my *public* key

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCcq+Ju/SsWVpigXx8kOZQ6OIoIaxDGRW9ew/u9XP9nCrDOTsKmKWtvCMVFTkNTLTgoKGrdOZqILGQ69pEddR5qKG8hzvqlBV+4C66CY48MhGn6Foitt/6zqYyqQYAcxMt2B0d9U+dbgRHYxUGyK+fILK7h/8/CvqyXOrL+jtnszQIDAQAB

Now that you know that, if you go here <https://www.devglan.com/online-tools/rsa-encryption-decryption> you should be able to decrypt my message (as usual add it to the file you’ll submit).

Now what’s interesting is although you can read this message, you can’t create a new message encrypted the same way. The reason is that when I made that ciphertext, I encrypted it with my private key not my public key. Messages encrypted with the private are decryptable with the public. Normally, I would publish my public key someplace really obvious. That means messages encrypted by my private key are really easy to decrypt.

Why would I want that? Well encryption by the private key is considered to be \*signing\*. That is, if you found another message that was decryptable by the same public key, you’d know that they were from the same person. No one else could have forged the message, because to do that they’d have needed the super-secret private key. Encryption by private key isn’t so useful for secure communication though.

The main reason I’d want my public key public though, is it makes it possible to send messages to me.

## Step 2b: Asymmetric Encryption – Key Exchange & Secure Communication

Ok now generate a key for yourself. Go here <https://www.devglan.com/online-tools/rsa-encryption-decryption> and press the “Generate RSA Key Pair Button”. You’re going to use this with the others in your breakout room. Pick one other member of your room that’s your “special friend”…make sure that everybody has a special friend. Your goal is to communicate to the special friend and back without it being possible for other members of your breakout room to overhear. BUT you can only communicate via Zoom breakout room chat – no other mechanism will be allowed.

Here’s how – have your special friend post their *public* key in the breakout room chat. Then, compose a message to them where you reveal your secret information (favorite color – nothing truly secret or bad ok?). Using the website, encrypt a message with their public key. Post that message in the public chat. They should put that message into the website and decrypt it with their private key. Messages encrypted with the public key can only be decrypted with the private. Now they should know your secret information.

They’ll want to send you a secret response. Post your public key in the chat. They should send you an encrypted message – decrypt it with the private key. Viola! You have just securely communicated.

To celebrate, compose a message to me explaining your excitement at securely communicating. Use my key from 2a to ensure only I can read it and put it in the text file.

If you are attempting to do this activity asynchronously, you only need to do that last step.

## Step 3: Betrayal & Man in the Middle

In this step I reveal that I have dishonestly used the vehicle of a 310 activity to discover all your secret information. My agent has been lurking in the breakout room chat this whole time. If all this agent could do is read your communication, it would be impossible for him to have discovered your secrets. However, my agent can edit messages that are sent in the chat, without the sender realizing the modification happened.

Discuss with your breakout room how my agent could have used this capability to discover all the secrets. Put your explanation into the text file.

## Step 4: Hybrid Systems

You might have noticed that symmetric encryption webpage offered you the opportunity to encrypt a file but the asymmetric encryption webpage did not. This is because asymmetric encryption is much more computationally expensive than symmetric encryption. But this turns out not to be a problem.

Discuss with your breakout room how you could safely send a large encrypted file to your special friend securely, without paying the high cost of encrypting the whole big file with asymmetric encryption. Assume that Zoom chat would allow you to send a large file AND that the issue discussed in Step 3 did not exist. Put your explanation into the text file.

## That’s it

Submit your file in the usual way. I hope you found this interesting!

Here’s my private key – not that’s it’s really useful for anything – but just so it doesn’t get lost if I need to modify this activity

