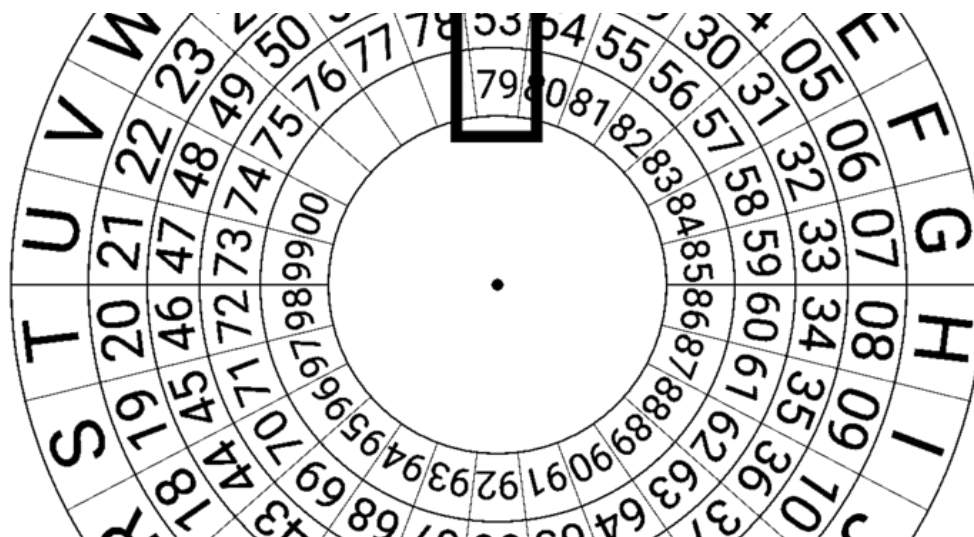




Search





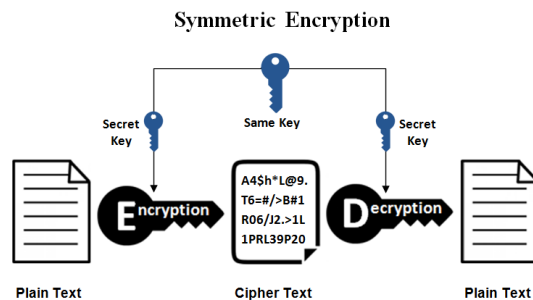
Search



VIEW the comments for more usage and ideas. You can go directly to the for ideas on how to communicate in an obfuscated manner that would be di SIGINT analysis while combining linguistic crypto.

What are Ciphers and why use them?

Ciphers are functions either through a form of math formulas or some other that can be repeated through steps. Ciphers are a small part of the world of where the primary goal is to hide messages or communications from people to know what you're saying. It also means you only want your messages to understood by your intended friend. Ciphers also reveal or unlock hidden messages through a key, something only yo and your friend know. Someone without he key cannot unlock the hidden message. As illustrated below, you take the method or steps you want to use to hide or encrypt the message and combine it with as secret (your key). Now the message becomes unreadable until your friend uses that same key to unlock or decrypt that the message:



To further explain for example, you wish to send your friend a message saying: "Are you online?" but you don't want your other friends to know. You use a cipher and a secret key to encrypt your message that scrambles it up, equivalent to a lock box. Your

other friends can't open the lock box of the real message because they don't have the key. The friend you sent the message to, will have your same key and then unlock the box to reveal the secret message you have sent. This is known symmetric encryption because you both use the same key to encrypt and decrypt the message.

Parents: Ask your child the difference between an encrypted message and a decrypted message?

Tip: Re-enforce the concept of the message in a lock box concept.

What is signaling and how are signals used?

Signals are any representation that "means" something to you or someone. For instance, speaking to someone, the set of noises and gestures you may make with face and hands all form one or more signals to your friend you're speaking to. When you write a message on a piece of paper and hand it to your friend, you are sending a signal, and your friend is receiving a signal. The signal is the piece of paper that transfers your message to your friend. You could send a different signal for the next message you want to send through by saying your message to your friend. If you write a letter to your friend, that's one signal. If you want to walk up to your friend and tell your friend something else or the same thing, that's another signal. Two distinct signals.



A Solution: You can also signal "YES" by nodding your head, or signal "NO" by shaking your head.

Putting it together: Using Word Search Puzzles for Crypto and Communicating Signals

Let's get hands-on with using ciphers and signals to communicate those hidden messages to our friend(s). Do you remember how a word-search puzzle works? You find words in a scrambled set of letters to reveal the messages someone wants you to solve. The following illustration is an example of a 15x15 square of letters with the followings that I may want to send to my friends! But before you go "solving" the word search puzzle; I want to communicate the phrase "change security" to my friend. But how do I hide it from anyone else seeing it but my friend?



OK I want to send "change security" to my friend without it easily been seen by other friends? Well we have to first use a cipher, as series of steps or math that will take "change security" and turn it into something not readable by anyone else but my friend.

Parents: Ask your child what components are needed to encrypt the message "change security" when I send it to my friend?

Solution: I will need the following components: my plaintext message = "change security", the cipher (steps to encrypt the message), and the secret key (to unlock the lockbox) for message decryption.

The Encryption Cipher of the Word Search Puzzle

Great! We have our components identified of what to use to send our message but how do we convert a word search puzzle into a cipher? We don't. The word search puzzle is an array of 2-dimensions (2D) is actually is the key you're going to give to your friend so they also have a copy to decode the message. We're also not going to "solve" the word search puzzle by circling the words. We're going to use what's called substitution and transposition as our *cipher*. Substitution is when you replace a character (letter) or word with something else in its place. A transposition is when you "shift" or "move" a character or word based on a specific offset interval.

A **combined** example of substitution and transposition cipher method is when you replace the letter "A" with the number "0" or the letter "B" with the number "1" and "C" with the number "2". We start with 0 because it's the offset, or position, of the English alphabet letter (26 letters total, but we start from position 0 that ends at 25). The substitution happens because A is no longer "A", it's represented by a number. The transposition happens because we're basing "A" based on its offset position of "0" because it's the start of the alphabet.




Search



...aining 1,2,3,etc. This is also known as a variant of the Caesar cipher, for example is specifically (ROT-0) which means rotation of 0. The original Caesar cipher was ROT-13.

How do we apply substitution and transposition as a cipher to the word search puzzle?

If we look at the word search puzzle as a 15x15 square, we can think of it as [quadrant](#) (Quadrant 4 specifically) from a math plane and assign each letter within as coordinate pairs. So the first letter in our puzzle, which appears to be "F" we can think of it as the pair, $x=0$, $y=0$ (0,0) because it starts at the first position (0 offset) for both the row and the column in the square. This is illustrated below:

 Now what would we do if we wanted to encrypt the word "fun" using our [word search](#) as the [key](#) and our [coordinate method \(substitution and transposition\)](#) as our [cipher](#)? Let's start off with the anywhere letter "F" appears.

Parents: Be sure to remind your child that it isn't important the "solve" the cross word puzzle with specific words, we're just using it as a shared secret key. If you were to have the child solve the puzzle by just finding words out of it, it defeats the purpose because it provides easy-plaintext readable messages that isn't obfuscated or encoded. **Tip:** If your child is wanting to focus on solving the word search, let them solve it. Then when they ask if it's encrypted or insist that it's encrypted; you refer back to the prior section on symmetric encryption and explain how another friend or parent could easily read their circled words on the page. Also remind them on the point of encryption (using ciphers) was meant for.

So we know one position of the letter "F" is (0,0) at the top left corner. Let's find and determine a position for the letter "U" and "N". Pick anywhere you wish!

Parents: Count from the (0,0) left position shifting right among the columns to find the column that that contains the letter you're looking for, "U". In this case we find that is still on the same row with column offset "9". Note this. Next, assist your child in determining the row offset, which is still 0 because it's at the starting line. Ask your child to repeat this themselves for the letter "N" any where on the puzzle. Remember in a coordinate display (X,Y) pair that X= Column, and Y = Row. To help with this concept consider running [my powershell script](#) with the appropriate [execution privileges](#) to further reinforce and guide your child. Be sure that you have PowerShell v3 or higher installed and set the Set-ExecutionPolicy bypass mode in your console. Note: I elected not to make a GUI program of this script because I believe it's important that new STEM professionals also become acquainted with CLI and text-only tools.



When running the PowerShell script ensure you enter the full path to the word search puzzle or put the PowerShell script in the same directly as example1.txt. Use a **CAPITAL "U"** when entering in the letter that you wish to help your child find appropriate coordinates.



Search



looking for. Ensure you explain this to your child carefully that this is how the computer displays a "false" or a "non-match" on your screen.

Tip and Solution Example: So after going through the word search array exercise of coordinate hunting you should have all 3 characters "fun" properly mapped to (x,y) coordinate pairs. Remember that column = x, and row = y. One solution is: F=(0,0), U=(2,2) and N=(5,4). If your child didn't a similar result or understand why it was "one off" based on offset. Review the previous section and look for the keyword "offset."

Parents: Have your child describe the components of the message "fun" using the word search puzzle encryption method.

Solution: Plaintext="fun" , Key=the word search puzzle itself, cipher to encrypt= finding the coordinate pairs of the letter we want to use. cipher to decrypt= matching the coordinate pair back to the word search puzzle as the key.

Parents: Now that we have successfully encrypted the plain text message "fun" how would we go about decoding (decrypting) the message using our key? Walk through with your child the components of the encryption process in reverse. Remember that the word search puzzle is the "shared secret" key. The cipher is the steps/methods of encryption and decryption. In our case, it is matching letters to coordinate pairs and back. Reinforce this concept to your child by asking them would someone who doesn't know the secret key and cipher be able to "decode" the message without telling them? (The answer should be: No, or Not Easily).

Extended Signaling and Cipher Concepts *Recommended for Grades 7 and above

By now you should have been able to successfully use symmetric crypto methods for encrypting and decrypting basic communications using a cipher, key, and plain text. We also discussed the idea of signaling which could include different mediums or channels by which your plain text, key, or encrypted text could be passed to a friend. What if you wanted to add on to this concept and further add complexity to your signaling. In a word-search puzzle, couldn't the shape be something other than a square? Couldn't it be a circle or triangle? When you utilize encrypted communications typically there are rotations that happen where the the friends communicating could change any of the following:

- The signal (e.g. voice, hand signs, winking, etc.)
- Cipher for encryption/decryption routines: (e.g. instead 1-1 coordinate matching to letters, what if you added a function of $2x+k$ where X is the plain text value substituted as an number (remember our discussion on Caesar ciphers?) and K is the key, where you could use any number). The output would be encrypted numbers that correspond to letters. For decryption you would use the inverse which would be the inverse function ($k - x / 2$).



Search



We have multiple components we can change to make it more difficult for outsiders to determine what you would tell your friend in an encrypted form. If we change the key, we usually can change the contents of the key or the size. In our previous examples, we used the word-search puzzle of a 15 x 15 square. To change the key means that I can use a completely different word search puzzle and letters all together. I can also change the size of the key space to be even bigger, 30 x 30. Overall, as long another friend or outsider **does not know all 3 parts (signal, cipher, and key)** of my secret communication or message; they cannot easily determine a message that I will send to my friend.

Parents: Ask your child how might changing the size of a key make it harder or easier for an outside party to determine the original message? Also ask your child if someone were to find out some or all of your communication parts, would they change any components of the secret communication, and why?

Solution: A change of the key size by growing the key makes the key space vast and require an outsider to look at more data to determine how the key is used (in our case a word search puzzle) and what messages are actually inside the key (again, in our case, a word search puzzle for 1-1 substitution and transposition US English alpha bet cipher). When you make the key smaller in our case, it narrows the total number of possibilities the decrypted or plain-text message could be. If one or more of your components within the secret communication is compromised (signaling, cipher, and key) it's best to change all 3 mechanisms so that the outside party snooping on your communication can't re-use any past knowledge to determine your new secret communication and messaging.

Alternative Signaling and Key Changes

The previous section(s) are about using common dialog that friends and people generally interact with each other. Signals can be sent over different mediums and meanings in more obfuscated ways. Have you ever thought about how radio and sound work? Sound travels in varying waves and frequencies. Different representations such as **sine vs. square** "wave" changes in sound and shape. In our example, we can apply a change in our signal representation to tell someone that the next key is going to be in the shape of a 15 x 15 square without actually speaking it in words. Your friend would already have to know the **signal protocol** which are a set of known "rules" for you both to communicate. You wouldn't necessarily communicate whole encrypted text messages to each other, but you will establish symbolic meaning using signals to share with each other the components of your secure communication (**key, cipher, and encrypted text**).

Let's go back to our original example of using a 15 x 15 square word search as our key. We already know that our cipher is based on a coordinate system on Plane 4 of a geometric 2D grid/array. Let's pretend that I want to tell my friend how the key will look like and what the key is. Rather than openly in plain-text communication tell them the exact key (such as handing them a copy of my word search or saying it out loud); why don't I use alternate



Search



Construct a 15 x 15 square as illustrated below.



I've highlighted the the notes that should be played based on the frames in a 15 x 15 pattern. My friend, who already knows my signal protocol would take the URL that I would send them that goes to my saved signal which represents the key space and shape that I will be using. If I had access to advanced technologies, I could also create a tool or device that takes the audio from the Song Maker here and re-illustrate it back as a square pattern representation visually.

To set up this 15 x 15 square, I need to ensure that the configuration of the song maker is set up for 3 octaves and enough bars to occupy the space as illustrated below:



After completing my 'saved' signal I can share it with my friend as a URL directly



from the [Google Music Lab](#) . Now my friend can receive the URL that represents my signal that this is how my secure communication key should be represented as.

You may be wondering what is the point of sending the "outline" of the key shape and space when you can't send the actual content of the key using our method from before. In this manner, you would augment the signal protocol's rule to also state "if sender bob sends a google music lab link to receiver jill, then also look at xyz location for the content of the key."

Such a rule would trigger the receiving friend to also go look at a second source, maybe a public one, for the actual content of the key. The person knows that the key is in the 2D array shape form of a square and is 15 x 15 according to our protocol. Let's say that the signal protocol directs the receiver to look at the [weekly or daily word search puzzle](#) as the key's contents. Now the sender and the receiver have established a shared secret key using public means and encoded signaling communications. The remaining piece of our secure communication is now the cipher that would be used. This cipher would either have to be communicated prior to secure communication out in the public *or* it would need to be communicated by adding more rules to the signaling protocol which also must be communicated between myself and my friend prior to our secure communication attempt.


Parents: Ask your child how using a word search puzzle as a key that changes daily or weekly might add extra work for both the outside parties trying to snoop or break the communication **AND** the sender and receivers of the secure communication? Ask your child how they could extend the signal protocol to incorporate and share their cipher steps using signaling as part of their pre-shared communication before attempting to establish a secure encrypted communication?




overhead to the senders and receivers by having to constantly "switch gears" and change their routines for secure communication. A weakness of symmetric encryption methods is that both sender and receiver must already know all aspects and components of the secure communication (signal, cipher, and key) to start with. Changing any component of the communication also increases the work an outside party has to do to essentially 'break' the encrypted text you're sending into something easily understood. That means they must know at minimum your signal, cipher, and key. The signal protocol can be extended by augmenting additional rules that describe (at least in our example) sounds, tones, or shapes that wouldn't represent the keyspace, but it would represent the key's content or a list of places to look for the key's content. This would be a form of substitution; however the distinction between signal and crypto substitution is that signaling is only substitution and always a 1-1 meaning (e.g. traffic lights, red, yellow, and green have the same meaning each time no matter what position they're in).

Changing the Cipher Function

In our previous examples, we have utilized the coordinate presentation as our system or steps to be our cipher for encryption and decryption routines in our secure communication. We can also easily implement substitution only cipher in the same symmetric key method. Our last method focused entirely on representing a geometric shape and the positions of each letter based on row and column. We can also use a simple math formula of $(2x+k)$ which would be our encrypting cipher function and $(k-x/2)$. X is our plain-text letter that represents a substituted character in the alphabet (could be 1-26) and K is our key.

 In the table above, we see that the offsets of letters A-Z range from offset 0-25. But unlike our previous example the offsets are **not** based on the 2D array which is our key (the square of 15 x 15 letters). Instead we utilize essentially ROT-0 as previously discussed where each letter corresponds to a 1-1 offset value. Now let's say we use a single constant of "10" to be our key instead. When plotting the graph function of $(2x+10)$ we get the following:

 Notice that that our encryption cipher function is $(2x+k)$, where $k=10$ which translates to $Y=2x+10$. So what do we enter for X ? X is our English alphabet offset number. So if I wanted to "encrypted" the word "fun" I would have to run the encryption routine 3 times: $(2*(5)+10)$, $(2*(20)+10)$, $(2*(13)+10)$ which gives respective encrypted ciphertext representation of "fun" as [20, 50, 46]. To decrypt you would pass the inverse function the encrypted characters as the following: $(20-10/2)$, $(50-10/2)$, $(46-10/2)$ which returns you back to the offsets 20, 50, 46 which translate back to "fun."

Parents: Try to experiment with different functions, something as easy as $(x+k)$ where x is your alphabet offset and k is your key number and having your child use it to encrypt, followed by the reverse function to decrypt. Stop to ask your child what is the cipher for encrypt, cipher for decrypt, and what the key is.

Wrap-Up Extra Learning and Challenges



Search



Learning within STEM. We have gone over some basic core concepts on what are signals, ciphers, and how to apply them using multi-dimensional arrays. For those of you with older children, the extended section reinforces the concepts of cipher use by changing components within the secure communication. Using symmetric key encryption methods, individuals can utilized pre-shared protocols, ciphers, and keys to create their own custom secure communication. We also learned that when you rotate or change any component of the secure communication that there is overhead on outside parties attempting to break or crack your secure communication.

Extra Challenge:

Using any combination of the above methods, can you think of a completely different signal, cipher, and key representation combination that could be used to established secure communications? Perhaps using 3-dimensional key spaces or a different signal protocol? Don't forget to try making your own word search puzzles for additional practice found at the [Discovery Education Channel](#) site.

Feedback:

I'm very much open to feedback if this or did not work for helping your child learn crypto and signaling. Please feel free to share or comment on how it helped or didn't help you. For those of you interested in cyber security and need services or products for your company or home, feel free to drop us a line at www.scissecurity.com We provide full cyber security stack solutions and utilize our own STEM skills to incorporate machine learning and other predictive analytics in hunting for threats within your environment.

[Report this](#)

0 Comments



Add a comment...

**Dennis Chow, MBA**

Cyber Security Consultant | USAF Veteran

More from Dennis Chow, MBA [See all 8 articles](#)

Healthcare Information Security
Professionals: The Future of Cyber...

Dennis Chow, MBA on LinkedIn

Using Signals Intelligence within
Cyber Security

Dennis Chow, MBA on LinkedIn

Auto Defending and Healing
Networks by Extending SIEM Value

Dennis Chow, MBA on LinkedIn

Static vs. Dyn
Explained

Dennis Chow, MBA on LinkedIn



Search

