LC4 Guide

General Info

LC4 permits only 36 symbols to be used, they are:

"#_23456789abcdefghijklmnopqrstuvwxyz"

You can swap them out for other symbols if you like, but make sure the recipient has a matching set of tiles. Do not modify the numbers on the tiles. The author omitted '1' and '0' to avoid confusion with 'l', 'I', and 'o' in handwriting.

LC4 makes use of a marker and a 6x6 grid of tiles, the page containing these should be printed out and cut into evenly sized squares. Doing this without them would be exceedingly tedious. Anything will suffice for a marker, provided it can sit on top of a tile without obscuring it. Because shuffling and manipulating pieces of paper is tedious, it may be worth using these as stickers on scrabble pieces or printing them on card.

Preparation

Do this once per recipient. While the same key+signature can be shared with multiple people, if one of them is compromised then your communication with all others will be too.

Choose & Share a Signature with the Recipient

Signatures aren't anything special, they just can't be known to the adversary. Their only function is to check if the ciphertext was altered during transmission, if it was then the signature will not match what it should be. They should be ≥ 10 symbols long and do not need to be random, but that would make them harder to guess. If the signature is known, it means your messages might be altered during transmission. Secretly share this with the recipient. You will reuse this in future messages with that recipient until it becomes known to the adversary.

Generate & Share a Key with the Recipient

Shuffle the tiles well, a good shuffle *really* matters. Lay them out in a 6x6 square. Read them off left-to-right and top-to-bottom and this is a key. Secretly share this with the person who will recieve your messages. You can reuse this for up to 46,000 messages with the recipient, if used for more messages the probability of the same nonce being generated twice is too high.

Encryption

Encryption is performed character-by-character, with each character becoming another. The grid and marker's position will be altered each time a single character is encrypted. To encrypt a sequence of characters, encrypt each character in it from left-to-right. We will call the unencrypted character the plaintext character, and the encrypted character the ciphertext character.

1. **Find the ciphertext character from the plaintext character according the the marker's tile's numbers**
   (a) Find the plaintext character in the grid.
   (b) From that tile, count to the right the number of tiles shown at the right of the tile under the marker. If you reach the end of the row, continue to the leftmost tile of the same row.
   (c) From this new position, count down the number of tiles shown at the bottom of the tile under the marker. If you reach the bottom of the column, continue to the topmost tile of the same column.
   (d) The tile you have found in this way is the ciphertext character, write it down unless you're encrypting the nonce.
2. **Right-rotate the plaintext row** Find the plaintext character in the grid again, shift every tile in that row one position to the right (with the rightmost tile moving to the now-empty leftmost position). This may cause the marker to move, this is ok.
3. **Down-rotate the ciphertext column** Find the ciphertext character in the grid, shift every tile in that column one position downwards (with the bottommost tile moving to the now-empty topmost position). This may cause the marker to move, this is ok.
4. **Move the marker according to the ciphertext tile's numbers** From the tile the marker is currently on, move it right by the number of tiles shown on the right of the ciphertext tile and then down by the number of tiles shown on the bottom of the ciphertext tile. If you reach the end of a row or column, continue counting from the start of the same row or column as before.

Decryption

Decryption is almost the same as encryption, only step 1 differs. Procede as normal, but during step 1 you will know the ciphertext character already and need to find the plaintext character. Find the plaintext character from the ciphertext character according to the marker's tile's numbers by counting left from the ciphertext character the number of tiles shown on the right of the tile under the marker, and then counting up from there the number of tiles shown on the bottom of the tile under the marker. Wrap back to the start of the same row/column as usual if you would otherwise move off the edge.

Sending a Message

1. **Generate a nonce** Shuffle the tiles well, draw one and write it down, place it back into the pile. Repeat until you have ≥ 6 symbols. Do not reuse this.
2. **Lay out the grid** Using the key you have previously secretly shared with the recipient, lay out a 6x6 grid from left-to-right and top-to-bottom. Place the marker on the top-left tile.
3. **Encrypt the nonce** Don't write down the ciphertext this produces, the point of this step is to mix up the grid.
4. **Encrypt the plaintext** Write down the ciphertext this produces.
5. **Encrypt the signature** Append the ciphertext this produces to the ciphertext produced in the previous step.
6. **Transmit** Transmit the unencrypted nonce, and then the ciphertext. Neither are secret.

Recieving a Message

1. **Lay out the grid** As above.
2. **Encrypt the nonce** As above. Note that you encrypt the nonce, not decrypt it, because you already know it. It is transmitted unencrypted and is not secret.
3. **Decrypt the ciphertext** Write down the plaintext this produces, this will be the original message followed by the signature.
4. **Check that the signature is correct** If the signature is not as expected then discard the message as it was corrupted during transmission.

Caveats

If a plaintext/ciphertext pair is known to the adversary, they can derive your key (still a lot of effort, but doable) and know your signature. Change both.

Example

Key xv7ydq#opaj_39rzut8b45wcsgehmiknf26l
Signature #rubberducky
Nonce bw6ib7
Plaintext this_is_a_test_of_lc4
Ciphertext r3qicv_iypnlnywas3_qn#rwmtwlwhwuu

# 0 0	_ 1 0	2 2 0	3 3 0	4 4 0	5 5 0
6 0 1	7 1 1	8 2 1	9 3 1	a 4 1	b 5 1
c 0 2	d 1 2	e 2 2	f 3 2	g 4 2	h 5 2
i 0 3	j 1 3	k 2 3	l 3 3	m 4 3	n 5 3
o 0 4	p 1 4	q 2 4	r 3 4	s 4 4	t 5 4
u 0 5	v 1 5	w 2 5	x 3 5	y 4 5	z 5 5