

What is Crosshairs? A manual encryption tool to assure the privacy of very short messages. What do I need? Just this document and some pencils. How does it work? A circle of trust is formed between 2 or more people. They first exchange physical paper keys securely in person, and later use them to “lock” (encrypt) messages manually on paper. Encrypted messages are then sent electronically. No one outside the circle of trust can intercept the messages. Why use this? In high-risk situations such as missions work, personal or operational details could endanger lives if intercepted. Electronic systems can be compromised in unpredictable ways. Physical paper is simple, private, and easier to control. Use for meeting locations, travel details, by-name prayer requests, uncensored personal notes, or whenever an electronic record is undesirable: PINs, etc. Is it difficult? The process is quite easy, but slow. Messages are limited to 30 characters and the number of messages is limited. Expect 2-5 minutes to process one message. Sample messages: JOHN-ARRIVED-SAFE PASTORARRESTED-USENEWLOCATION MEET-312BROADST-JUL31-NOON PVG-TERM2-BROWNSUITBLUEFLAGHAT	Is it reliable? Yes! It is 100% immune to code breaking via interception. This is a mathematical truth and not dependent on current technology or society. It is also immune to hacking or any digital exploit, since it relies on pen and paper. Why should I trust it? You should not trust this method blindly but instead understand and convince yourself <i>why</i> it works. Full understanding will also help ensure you apply the process correctly. So, why is it unbreakable? The underlying principle is known as the One-Time Pad cipher, which you may research yourself. A brief outline follows here. Sender and receiver(s) previously agree on a shared secret list of random numbers (called the key) to be used to transform the message (called plaintext) into unreadable gibberish (called ciphertext), and then transform the ciphertext back into the original plaintext. Each character in the plaintext gets scrambled by the corresponding secret number from the key, across all possible character values. If a spy intercepts the ciphertext, they have no way to tell if it originally said "please help" or "everything ok" or "send cookies", because each could equally well have yielded the exact same ciphertext, determined completely at random by the key. Without the key every conceivable message is a valid possibility. The only way to know the true message is to know the true key, and there's not even a way to know whether a given key is "true".	Furthermore, since the single-use key is only used once - each character scrambled by its own dedicated random number - there exists no insight to be gained from any analysis of the scrambled ciphertext. It is random gibberish. The only thing apparent from the ciphertext is the maximum possible message length. The bottom line is that without the key the message is simply absent from the ciphertext, in a deeply philosophical and mathematical way. All of this assumes a truly random key, where each number is equally likely and no number influences subsequent numbers. In other words, 100% unpredictable. It is therefore important to create keys from a trustworthy source of unpredictable and uniformly probable randomness. Mentally generating numbers is not recommended. How does this tool apply the above principles? The message is first translated into pairs of digits. This is merely to put the plaintext into a workable form and does not contribute to security. The actual encryption, then, deals only with numerical digits and doesn’t know about letters. The encryption or decryption happens one digit at a time via a number square, scrambling the plaintext digit (row) according to the corresponding key digit (column). The number square is designed for efficiency, while maintaining the crucial property that each row has every digit 1 through 6, and therefore each plaintext digit gets properly scrambled across all possibilities.	Additional Tips and Enhancements <i>Mental Signature</i> Memorize but don’t write down a unique ordering pattern for the 30 cells when copying encrypted digits, rather than standard left-right top-down reading order. Helps identify sender impersonation if key is stolen or sender is coerced. Note: does not prevent message interception if key is stolen (but it does help). <i>Biometric Seal</i> Store keys in opaque envelopes and seal with traditional sealing wax stamped with thumbprint until ready to use. Adds confidence that keys are original and kept private. <i>Layered Encryption</i> Encrypt with one key, then encrypt <i>those</i> digits with another key. Useful to ensure two people working together to send and/or receive. Encrypted message secure unless both keys compromised. <i>Hide Existence of Messages</i> Ciphertext can be hidden in various media to conceal that a message exists. Hidden ciphertext need not be sent to recipients but can be published anywhere. As appropriate, convert digit pairs to letters/numbers via table map and use uppercase/lowercase/mixed. Suggestions: - URLs: many contain Base64 parameters that can be changed without breaking the link. For example a URL to share a YouTube video may look like: https://youtu.be/aBCdEFg?si=hiJkLmNopQRsTuvw where the part after si= can be silently replaced with ciphertext. - Filenames: e.g. “download_hiJkLmNopQRsTuvw.png”. - Lot Numbers: write ciphertext on some product, then capture in photo. E.g. “Lot No. MWXRO8N22A”. - Text: write or edit some text so number of words in each sentence corresponds to a ciphertext digit. Count in a circle looping back to 1 after 6. To encode 2 the sentence could have 2, 8, or 14 words, etc. Very tedious but extremely effective.
--	---	---	--

2nd

	1	2	3	4	5	6
1	₁ –	₂ A	₃ B	₄ C	₅ D	₆ E
2	₁ F	₂ G	₃ H	₄ I	₅ J	₆ K
3	₁ L	₂ M	₃ N	₄ O	₅ P	₆ Q
4	₁ R	₂ S	₃ T	₄ U	₅ V	₆ W
5	₁ X	₂ Y	₃ Z	₄ 1	₅ 2	₆ 3
6	₁ 4	₂ 5	₃ 6	₄ 7	₅ 8	₆ 9

Footnotes:

1Get pack of 6-sided wooden pencils, write digits 1-6 around shafts. Shuffle handful, spread on flat surface. Alternative: cubical dice in transparent compartment box. Shake box.

²Duplicate by hand or via carbon transfer paper. Tracing may work if paper is thin. Do not use electronic photocopiers.

³For numbers in message: O = zero, P = point, N = negative.
Example: -5.03 = N5PO3

5, 4 1	5, 5 2	5, 6 3	6, 1 4	6, 2 5	6, 3 6	6, 4 7	6, 5 8	6, 6 9	
3, 6 Q	4, 6 W	1, 6 E	4, 1 R	4, 3 T	5, 2 Y	4, 4 U	2, 4 I	3, 4 O/Ø	3, 5 P
1, 2 A	4, 2 S	1, 5 D	2, 1 F	2, 2 G	2, 3 H	2, 5 J	2, 6 K	3, 1 L	
5, 3 Z	5, 1 X	1, 4 C	4, 5 V	1, 3 B	3, 3 N	3, 2 M			
1, 1 -									

Instructions

Prepare and Distribute Keys

1. Print copies of single-use key sheet. For each future message to be sent, a specific sender is assigned, and sender and recipient(s) each need 1 copy. E.g. if 2 people then 4 copies allow for 2 messages each pre-assigned. Also print 1 copy of these instructions per person.
2. Secure privacy of environment and remove cameras and imaging devices.

For each message, duplicate² the following across all copies for that message:

3. Write Sender name to assign to specific person.
4. Get random 6-digit ID with pencil dice¹ and write next to ID & Data.
5. Each of 30 cells in key sheet has 2 number squares. Each square needs own random digit. Generate digits with pencil dice¹ and draw vertical lines to right of number in top row. Example for 3 and 5:

1	2	3	4	5	6	1	2	3	4	5	6
2	1	5	6	4	3	2	1	5	6	4	3
3	4	1	5	6	2	3	4	1	5	6	2
4	3	6	1	2	5	4	3	6	1	2	5
5	6	2	3	1	4	5	6	2	3	1	4
6	5	4	2	3	1	6	5	4	2	3	1

6. Fill all 30 cells with uniquely random digits: 60 digits in total.

7. Distribute keys to people so each has 1 sheet per message. Identical sets of papers between people. Do this securely by meeting in person.
8. Everyone must guard their keys and keep them private.

Encrypt and Send Message

1. Secure privacy of environment and remove cameras and imaging devices.
2. Find a single-use key sheet with your name as Sender.
3. Use above table or keyboard map to convert message³ to digit pairs.
4. Underline rows for digit pairs in each cell. Example for **M**:

1	2	3	4	5	6	1	2	3	4	5	6
2	1	5	6	4	3	2	1	5	6	4	3
3	4	1	5	6	2	3	4	1	5	6	2
4	3	6	1	2	5	4	3	6	1	2	5
5	6	2	3	1	4	5	6	2	3	1	4
6	5	4	2	3	1	6	5	4	2	3	1

5. Proceed in reading order (left-to-right, top-to-bottom) through key sheet. Add extra dashes (1, 1) at end to disguise length of message.
6. Crosshairs point to encrypted digits via top-left quadrant. In example they are 1 and 4.
7. Copy encrypted digits to solid line at bottom of key sheet.
8. **IMPORTANT:** Tear where indicated and destroy top part.
9. Transmit ID & Data to recipient electronically: text, email, photo, etc.

Receive and Decrypt Message

1. Secure privacy of environment and remove cameras and imaging devices.
2. Find single-use key sheet whose ID matches first 6 digits received.
3. Underline rows for remaining digits. Digits from the example (see left) are 1 and 4:

1	2	3	4	5	6	1	2	3	4	5	6
2	1	5	6	4	3	2	1	5	6	4	3
3	4	1	5	6	2	3	4	1	5	6	2
4	3	6	1	2	5	4	3	6	1	2	5
5	6	2	3	1	4	5	6	2	3	1	4
6	5	4	2	3	1	6	5	4	2	3	1

4. Proceed in reading order (left-to-right, top-to-bottom) through key sheet.
5. Crosshairs point to decrypted digits via top-left quadrant. In example they are 3 and 2.
6. Lookup digit pairs via above table map to recover message³.
In example 3 and 2 maps to **M**.
7. Write message on solid line at bottom of key sheet.
8. IMPORTANT: Destroy key sheet after reading message.

