

Instruction Reference Sheet

See page 4 for literature on the topic.

How to Prepare Keys

Prepare Pencil Dice:

1. Get some six-sided wooden pencils.
2. Use marker to write **1,2,3,4,5,6** around shaft faces.
3. Use in next section to generate random digits: shuffle in hand, spread on flat surface, read face-up digits.

Tip: orient pencils horizontally and place above page for comfortable shuffling.

Generate Keys:

1. Print copies of single-use key sheet. Sender and recipient(s) will each consume one per message.
2. Secure environment. No cameras, etc.
3. Assign Sender and six-digit random message ID. Sample:

Sender: *Robert*
ID & Data: **623153**

4. In each cell draw a horizontal line through the dots for a random digit. Sample '5':

54321MNBVCXZ876LKJHGFDS	123456123456
876LKJHGFDSA-9POIUYTREW	1.....4.....
-9POIUYTREWQ54321MNBVCX	2.....5.....
54321MNBVCXZ876LKJHGFDS	3.....6.....
876LKJHGFDSA-9POIUYTREW	

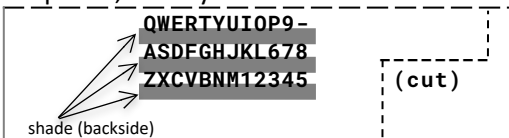
5. In each cell draw a vertical line to the **right** of a random digit down through the horizontal line. Sample '3':

54321MNBVCXZ876LKJHGFDS	123456123456
876LKJHGFDSA-9POIUYTREW	1.....4.....
-9POIUYTREWQ54321MNBVCX	2.....5.....
54321MNBVCXZ876LKJHGFDS	3.....6.....
876LKJHGFDSA-9POIUYTREW	

6. Each cell must have two intersecting lines, each its own dedicated random digit.
7. Duplicate entire sheet by hand (no photocopies) so sender and recipient(s) each have identical copy.

Tip: carbon transfer paper makes duplication easy and reliable. Improve by shading backside of number region with crayon

8. Heavily shade **backside** of keyboard grid with pencil, colored pencil, or crayon:

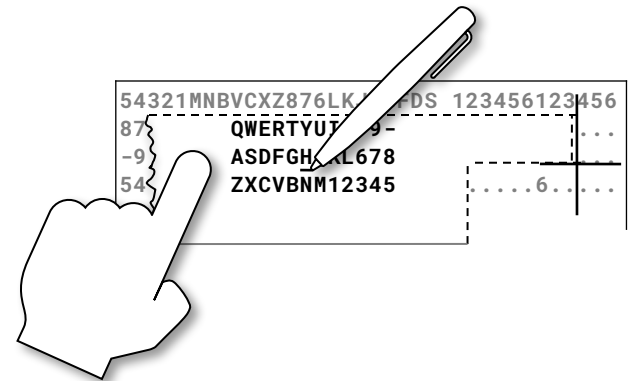


9. Cut along dashed lines and discard bottom-right corner of page. Cut along top dashes but do not tear off yet.

10. Meet securely in person to distribute keys so sender and recipient(s) each have identical sets.

How to Encrypt and Send Message

1. Secure environment. No cameras, etc.
2. Find a key with your name in Sender field.
3. Tear off keyboard grid where indicated.
4. Place on top-left key cell.
5. Align cutout corner to intersecting lines. Hold in place.
6. Underline desired character using ballpoint pen.



7. Slide keyboard down column cell by cell, aligning cutout and underlining next desired character.
 - a. Do entire 1st column, then 2nd, etc.

8. Shading-transfer underlines show encrypted characters:

54321MNBVCXZ876LKJHGFDS	123456123456
876LKJHGFDSA-9POIUYTREW	1.....4.....
-9POIUYTREWQ54321MNBVCX	2.....5.....
54321MNBVCXZ876LKJHGFDS	3.....6.....
876LKJHGFDSA-9POIUYTREW	

9. Write encrypted message in ID & Data, copying from same top-down column sequence.

Sender: *Robert*
ID & Data: **623153 4...**

10. Remove message cell (tear or cut).
11. Destroy key sheet and keyboard grid.
12. Transmit ID & Data to recipient(s).

How to Receive and Decrypt Message

1. Secure environment. No cameras, etc.
2. Find key with ID matching first six digits received.
3. With remaining received characters, follow same Slide-Align-Underline process as above.
4. Shading-transfer underlines will be original message.
5. Destroy key sheet and keyboard grid.

Introduction and Literature

What is Slipkey?

Slipkey is a pen-and-paper tool for protecting very short messages when electronic devices are the wrong tool for the risk.

The point is direct human control. No phone, computer, or app ever sees the plaintext message. Additionally, the encryption itself is mathematically bulletproof: unbreakable by interception and analysis. Encrypted messages are un-hackable and un-breakable.

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?

Use it when a message is short and the privacy risk is high enough to justify a slow manual process: meeting locations, travel details, names, emergency status, short instructions, PIN-like values, or uncensored personal notes.

The encrypted text can travel through ordinary channels. The channel does not need to be secret for message content, though it may still reveal who communicated, when, and how often.

Limitations

This protects message content from code breaking. It does not hide metadata, prevent coercion, protect a photographed or stolen key, authenticate the sender by itself, or save a plaintext that was exposed to a device or camera.

It is slow and short by design. It is also unforgiving: reused key material, guessed random numbers, copied keys, unclear cell order, or sloppy destruction can defeat the security.

Why is it unbreakable?

The keyboard supports 36 characters: A-Z, 1-9, and dash. For each message character, the key randomly chooses one of 36 possible alignments, which maps the input character to 1 of all 36 possible characters. In other words, it scrambles it across all possibilities with uniform probability. Every plaintext character could have produced the same ciphertext depending on the key.

A full message works the same way when every character has its own dedicated fresh random key value.

From the outside, this means that with an intercepted ciphertext, guessing the message is no better than guessing the key. If the key is random, then guessing either is impossible. Cracking the plaintext by interception and analysis of the ciphertext is simply not possible.

How does the grid scramble characters?

Each cell uses two random digits from 1 through 6, selecting one of 36 alignments for the keyboard grid. The printed layout hides the arithmetic: align the cutout corner to the crossing, underline a visible character, and the shaded back transfers the mark to its paired character on the key sheet.

The important properties are: each alignment can produce every supported output exactly once, the mapping is reciprocal, each cell gets its own independent random alignment, and used cells are destroyed.

Confidence check

You do not have to trust the layout blindly. On a test copy, choose one character such as A and try all 36 crossings. The transferred results should include every supported character exactly once. Then test reciprocity: if A transfers to T at one crossing, T should transfer back to A at the same crossing.

Handling rules

- Print blank sheets freely, but never photocopy, scan, photograph, or electronically duplicate completed key material.
- Generate random digits physically. Do not make them up mentally or reroll because a result looks wrong.
- Use every key sheet once. Destroy the entire used sheet, including unused cells.
- If message length is sensitive, agree on padding so messages appear the same length.

Optional enhancements

A private mental cell order can help detect impersonation if a key is stolen. Opaque envelopes, wax, tape, thumbprints, or handwritten marks can make casual tampering more visible. Two-person control can be added by encrypting once with one key and again with a second key. If the existence of ciphertext is dangerous, conceal only the ciphertext after encrypting on paper.

Summary of Rules

Random keys. Secret keys. One use. Destroy after use. If all of those requirements are met, the message is securely protected.

“Come to me, all you who are weary and burdened, and I will give you rest.” –
Matthew 11:28