MEPAK

'M'anually 'E'ncryption with 'P'artially 'A'lternating 'K'ey

WWW.MEPAK.DE

COMPONENTS

-MEPAK Board to snap the plates
-Storage Boxes for Key Plates A-Z and a-z
-2 Letter Plates on top with multiple Key Modifier Columns
-104 wooden Key Plates. Rotatable and flippable, 416 different variations.

USAGE

Secure encryption of messages without risk of using insecure electronic devices.
There are a lot of critical elements in using electronic devices of any kind, there are keyloggers operating in background, backdoors in chips, corrupted routers and connections and the more complex technology goes the less we understand the entire data flow. MEPAK offers a save and technology independent way to manually encrypt short text messages.

RANGE OF APPLICATIONS

-Teaching / learning how cryptography works at school or at home.
-Having fun sending manual encrypting message with friends
-Use it to send encrypted messages

HOW TO USE

Place the first Letter Plate marked with a single engraved cycle at the top inside the MEPAK board, the cycle is on top and left top side. Lay the second Letter Plate marked with the concentric double cycles at the top right side nearby the MEPAK board.
Create a new key or place the key tokens as an existing key defines. Each key have a unique name noted at the right side. You can rotate and flip every key plate to represent 4 different keys in total, for example A1, A2, A3 or A4.
Capital and small characters are different, a2 is not identical to A2.

After mounting all key plates choose the first character you want to encrypt at the bottom, follow the line to the top and write down the crypted character you see there. This is the first encrypted character of your message.

Then process the Key Modifier Column above from top to bottom:
-45: two numbers: Exchange the Key Plates with the corresponding numbers.
-F4: Flip the Key Plate this specific number to the backside by rotating about the length axis.
-R4: Rotate Key Plate with the specified number clockwise.
-LF: Flip Letter Plate to its other side.
-LR: Rotate in this case means to exchange the Letter Plate with the second Letter Plate nearby the table. Don´t flip or rotate it.
-4: (single number) add this amount of random characters to your encrypted text. They variate the length of the encrypted text. During decryption strikethrough the next given number of characters and ignore them during translation further letters.

Then continue with the next character the same way.
Decrypting needs works exactly the same way but you chose the character at the top and follow the line to see and note the decrypted character at the bottom A-Z line.

I also explain it in videos shown at WWW.MEPAK.DE

FAST MODE

For beginning and encryption which should withstand only manual decoding attempts you can use the Fast Mode.
To do so only process the bottom 3 Key Modifiers and ignore the modifiers above.
Do withstand even up to date digital brute force attacks you should use the Normal method using the entire Key Modifier Colum.

PASSWORT GENERATION

You may define a easy to remember password by using fantasy words and mix them with numbers following a fantasy rule you defined and can easily remember for example: **sumGISAmoO** with the numbers **8866543212** which result in: **s8-u8-m6-G6-I5-S4-A3-m2-o1-O2**

SECURITY ADVICES

A key generated by using 10 of 104 Key Plates each with 4 different positions results in 9,9,E+25 possible combinations.
I concepted this system save but only the reality and experts can proof it. So I cannot guarantee safety but I will call out a contest with a prize to proof its safety. And this prize will be increased the more people supporting and donating this project.
I guess a brute force attack need to calculate the first 10 characters with any possible key and check if it result in a valid text result. I estimate that will need at least 200-1000 operations per key, 1,98E+28 operations needed in total.
A High End Graphic Card (2020) with 1,2E+13 operations per second will need around 50-250 million years to finish this calculation.
Using further tips even increase the security level:
-I strongly commend to use a couple of random characters at the beginning and end of every message.
Try to avoid writing multiple messages with exactly the same text at the same position specially if placed right at the beginning. That´s why a pre attached combination of random characters at the beginning increase the safety. That was the reason for a weakness of the ENIGMA system during world war two, they used to send a standard set of data like the weather info at the beginning of each message in exactly the same way.
-Please store all Key Plates right after usage in alphabetical or a chaotic order inside the storage boxes and do not store the plates of your key all together at nearby slots.

EXTREME SECURITY

If you still want to increase the cryptographic strength you can take care the following things:
-A strong way to increase security is to use a second Key Modifier Column as well, for example:
Use the character specific Key Modifier Column and the right side nearby column as well. Or use the column 3 columns left the basic column as well etc.
-Don’t use “-“ as empty space between words.
-Use short words in your text, do not spell correct and try to avoid free spaces"-".
-Create own Letter Plates and share a physical copy with the people you want to communicate with.
-For ultimate security create and use additional own made Key Plates.

PRIZE CONTEST

To proof the safety of this system I decide to use MEPAK to encrypt a text and the first who decrypt it without knowing the password will win a prize money of **$200** (US dollar).
I used a standard 10 Key Plate Password but only the SECURITY ADVICES and no EXTREME SECURITY OPTIONS. Please help me increasing this prize by donating, or just honor this project, or get the prize for your own by solving it! The encrypted Message is:

AM42MSOH-X6P0430QALY4PDICBYMX0OZS0LLR1N62GB7Z0HH4L25U1M5NPMMFW0UO5SZYPC9HUP

MEPAK can be downloaded, emulated for own usage by using the digitalized content of it see attached file or ordered via e-mail with discount for educational usage and bigger quantities.