"Walk-in-the-Park" Cipher CoEncryption *(Illustration)*

US Patent 6,823,068

BitMint, LLC

The Walk-in-the-Park (WaPa) cipher is readily disposed towards co-encryption, as illustrated herein. Let Zachary be using a three letters alphabet X, Y, and Z, in which he writes one message for Alice: M_a = YXZZYXXZ and another message for Bob: M_b = ZXYYXYZ. Zachary wishes to co-encrypt these messages into a single ciphertext C:

$$C = CoEnc(M_a, M_b, K_a, K_b)$$

Such that Alice using her key, K_a, will decrypt C to M_a, and Bob, using K_b will decrypt the same ciphertext to his message M_b:

$$M_a = Dec(C, K_a); M_b = Dec(C, K_b)$$

Using WaPa, Zachary designates a rectangular array with a starting point, and marks its squares with the four letters: X, Y, Z, W -- one marking constitutes Alices' Key, K_a, and the other constitutes Bob's key K_b.

W	W	W	W	W	W	W	W	W	W
W	Z	Z	Z	Z	W	W	W	W	W
W	X	W	Y	Y	W	W	W	W	W
W	X	X	X	X	W	W	W	W	W
W	W	W	W	W	W	W	W	W	W
W	W	W	W	W	W	W	W	W	W
W	W	W	W	W	Y	Y	Y	Z	W
W	W	W	W	W	Y	Y	W	Z	W
W	W	W	W	W	Y	Y	X	X	W
W	W	W	W	W	W	W	W	W	W

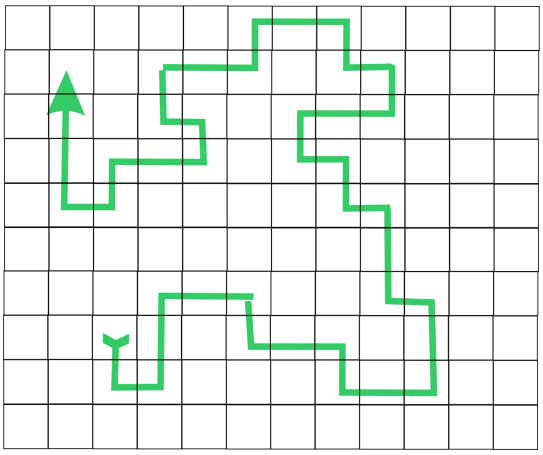
Alice's "Park" (key)

W	W	W	W	W	W	W	W	W	W
W	W	W	W	W	W	X	Z	Z	W
W	W	W	W	W	W	X	W	Y	W
W	W	W	W	W	W	Y	Y	Y	W
W	W	W	W	W	W	Y	Y	Y	W
W	Y	Y	Y	W	W	W	W	W	W
W	Y	Y	Y	W	W	W	W	W	W
W	Y	W	X	W	W	W	W	W	W
W	Y	Z	Z	W	W	W	W	W	W
W	W	W	W	W	W	W	W	W	W

Bob's "Park" (key)

Given these two keys Zachary marks a single pathway on the "park" (the keys):

The pathway is completely defined through its steps taken from the starting point. Using U, D, L, R to denote Up, Down, Left, Right the pathway is fully defined by the following sequence, which represents the co-encrypted ciphertext C:



The Marked Pathway (The Ciphertext)

C =

DRUURRDRRDRRUULUULULURRULU

LLDLLLDRDLLLDLUUU

When Alice marks the ciphertext C on her key she extracts the following sequence:

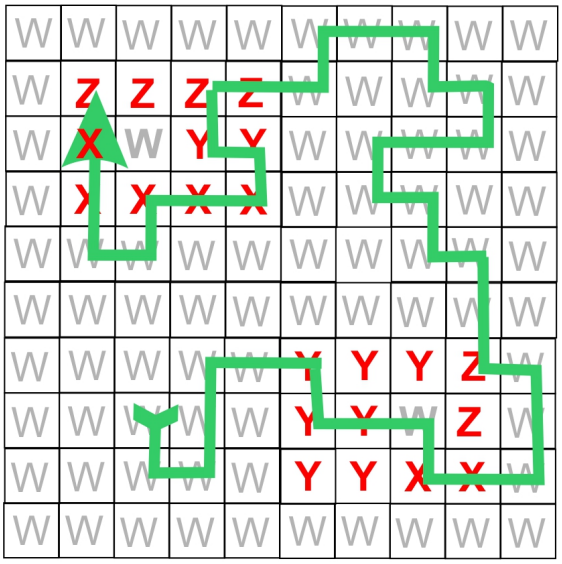
M"$_a$ =

WWWWWWYYYWXXWWWZWWWWWWWWWWWWWWZZYY

XXXWWXXZ

Alice then removes all the repetitions from the sequence:

M'$_a$ =WYWXWZWZYXWXZ



Alice Decrypts the Pathway on her marked “Park” (key)

And finally she removes the W letters:

$$M_a = YXZZYXXZ$$

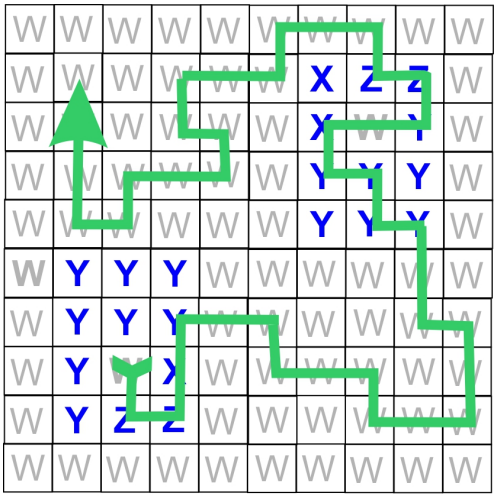
And she extracts the message intended for her.

Bob, on his part, overlays the very same ciphertext, C, over his "park" he reads a different sequence:

$$M''_b =$$

WZZXYWWWWWWWWWWWWYYYYXWYZZWWWWWWWW

WWW



Bob Decrypts the Pathway on his marked “Park” (key)

Here are C, M''_a, M''_b overlaid:

```
*DRUURRDRRDRRUULUULULURRULULLDLLDRDLLDLUUU  -> Ciphertext C
WWWWWWYYYWXXWWWZWWWWWWWWWWWWWWZZYYXXXWWXXZ  -> Alice's Plaintext
WZZXYWWWWWWWWWWWWYYYYXWYZZWWWWWWWWWWWWWWW  -> Bob's Plaintext
```

Next Bob shrinks all the repetitions: M''_b --> M'_b:

$$M'_b = WZXYWYXWYZW$$

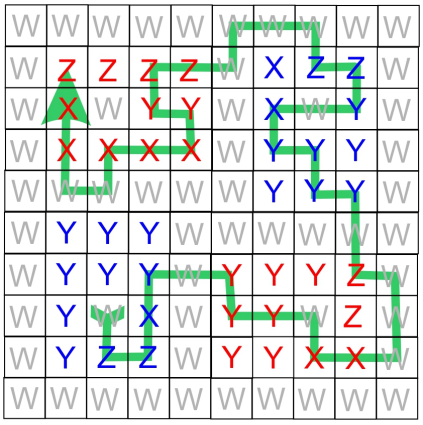
and from M'_b Bob extracts the message intended for him: M_b:

$$M_b = ZXYYXYZ$$

This demonstrates how Zachary creates a single ciphertext that is interpreted to two completely independent messages (or to two related messages). Neither Alice, nor Bob are aware that the ciphertext they have been decrypting also contains another message.

The same can be extended to any number of messages all co-encrypted into a single ciphertext. As discussed this feature lends itself to several powerful applications.

Zachary may also deal with Abigail (Abi) who gets both Alice's key and Bob's key. Using her key, Abi would read both Alice's and Bob's messages.



Abi Decrypts the Pathway
on her marked "Park" (key)

Note that while the keys in the illustration have been kept simple to clarify the process, these keys, will each serve to encrypt and decrypt any size plaintext.