The proof of the existence of perfect secrecy through all-way functions

The One-time pad offers fast all-way function based encryption with unlimited plausible deniability and guaranteed privacy. All-way functions are those with maximum reversal solutions not exceeding deductive reasoning given the key. Any guess key successfully decrypts all-way function based files and each guess key produces a different output making it impossible to say which output was intended by the key owner for that file. Brute force attacks produce plaintext with every possible symbol combination for that length. The following tables demonstrate all-way nature using modular arithmetic.

Ten-symbol addition possibilities of (a+b) mod 10

There are ten of each digit in the grid. Every column and row contains one of each digit. Every digit yields ten different digits. If only one value is known, the other two are unknown. If two values are known, the third can be logically deduced. There are 10^2 total outputs.

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Three-symbol addition possibilities

key symbol \ plaintext	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Similar rules apply for any number of symbols. Here, for every output symbol, three possible input pairs exist and this does not exceed deductive reasoning. For every guess key symbol, only one plaintext symbol is made responsible and for every guess plaintext symbol, only one key symbol is made responsible.

Encryption sample for ten symbols

The output stream borrows random information from the key therefore repetitive data does not degrade file randomness as shown where the plaintext repeats excessively.

random disposable key =	7	2	3	8	7	2	5	3	7	4	8	1	6	9	3	3	2	7	0	9	9	2	4	1	4	1	6	0	2	2
plaintext in base ten =	7	9	2	3	4	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0	9	4	5	0	5	3	7	4	9	
ciphertext output =	4	1	5	1	1	4	7	5	9	6	0	3	8	1	5	3	2	7	0	9	9	1	8	6	4	6	9	7	4	1

$(7+7) \bmod 10 = 4$

Privacy is guaranteed if random disposable keys are first shared in private. Users planning to share large files must first share significantly large key files in private. Whatever the stored or transmitted encrypted data, its contents cannot be related to you if your copy of the keys is destroyed. And anyone with keys who decrypt your data into something plausible or even illegal still cannot prove the intended output of your data.

Ten-symbol systems are said to have a plausibility ratio of 1:10 and three-symbol systems—a plausibility ratio of 1:3. This ratio may approach infinity and is calculated using the formula: 1 to number of symbols—or to be mathematical—number of symbols to number of symbols squared. Higher ratios compensate for weak random number generation.

The encryption sample for ten symbols demonstrates obfuscation of the fixed-length plaintext of 30 digits. The message itself may be less than or equal to 30 digits since any remaining space is dynamically filled with new random numbers. Had the key length been adjusted to match every plaintext length, the adversary would have a hint at what a short message could be. And had there been no random numbers appended to each message, key digits who drop to fill the remaining output space would give the cryptanalyst a closer look at the exposed key fragments and their generating algorithm.