5 Cascades of Different Ciphers

Examples

1. Monoalphabetic substitutions and transpositions commute. Combining more than one of each doesn't make sense since each of these two types forms a group. Composing one monoalphabetic substitution and one (simple) transposition makes a weak cipher. Solving it by a ciphertext only attack starts with a frequency count that reveals the most common letters.

2. The same remark applies to periodic polyalphabetic ciphers and transpositions. But if we take different period lengths for each step we get a fairly complex cipher, however it is too complex for manual operation.

3. The Enigma composed a monoalphabetic cipher with several polyalphabetic substitutions of different periods, followed by one more monoalphabetic substitution. The result was a single polyalphabetic substitution with a very large period.

4. The ADFGVX cipher used by the German army in WW I consisted of a substitution followed by a columnar transposition. For the substitution the 26 letters and 10 digits were distributed into a 6-by-6 square in an order defined by the key. Then each character was replaced by its coordinates in this square that were denoted by A, D, F, G, V, X. The French (Painvin und Givierge) had many successes in breaking this cipher.

5. Composing a monoalphabetic cipher with an autokey cipher is one of the "modes" that make block ciphers a little bit harder, see Chapter 3.

6. Finally recall that Porta's disk cipher had a representation as composition of a monoalphabetic substitution with a Belaso (aka Vigenère) cipher.

As a résumé we may state that cascades of different ciphers in general increase the security, but not always. In any case the situation requires a careful analysis before we trust a newly constructed product cipher.