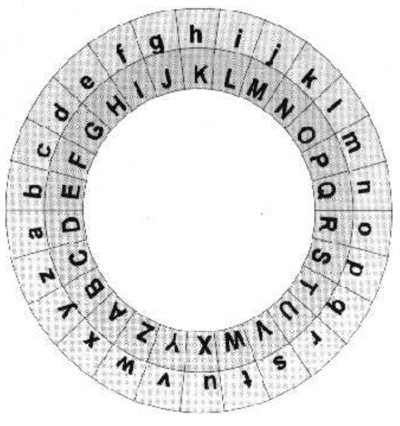
Geschichte der Kryptologie im Mittelalter

Im größten Teil des europäischen Mittelalters hat es keine nennenswerten Weiterentwicklungen der Kryptografie gegeben. Die im späten Mittelalter aufkommende Stärkung diplomatischer Beziehungen hat dann jedoch einige Fortschritte hervorgerufen. Die bekannten Techniken der Substitution und Transposition wurden verbessert, indem unnötige Buchstaben im Chiffrat eingefügt und zusätzliche Symbole (Punkte, Striche) verwendet wurden. Zudem wurde auch verstärkt *Steganografie* verwendet.

Bei der *Steganographie* wird versucht, eine Geheiminformation in einer harmlosen Nachricht zu verstecken. Damit wird nicht, wie bei der Chiffrierung, die Aufmerksamkeit auf einen kryptischen Text gelenkt. Das Schreiben mit Geheimtinte ist ein Beispiel für Steganografie.

Eine steganografische Methode wurde von Abt Johannes Trithemius (1462–1516) vorgestellt. Dabei wird jeder Buchstabe des Klartextes durch ein Wort im Chiffrat repräsentiert, so dass der verschlüsselte Text ein grammatikalisch korrektes Gebet ergab. Er beschrieb auch Substitutionstabellen, die es erlaubten, eine von einem Schlüssel abhängige Substitution zu verwenden.

Ein Meilenstein der Kryptografie geht auf Leon Battista Alberti (1404–1472) zurück. Er stellte mit seiner Alberti-Scheibe (1466) die erste polyalphabetische Verschlüsselung vor. Die Alberti-Scheibe besteht aus zwei konzentrisch angeordneten Scheiben, die jeweils ein Alphabet enthalten und die gegeneinander verdreht werden können (siehe Abbildung). Eine Stellung der Scheiben repräsentiert eine Substitution. Ein geheimer Schlüssel kann nun die Veränderung der Substitution beschreiben, z.B. „Drehe die Scheibe nach jedem zehnten Buchstaben um sechs Positionen im Uhrzeigersinn“. Mit Verwendung der Alberti-Scheibe werden traditionelle Häufigkeitsanalysen wirkungslos.



Der Franzose Blaise de Vigenère (1523–1596) entwickelte während diplomatischer Missionen beim Vatikan eine weitere polyalphabetische Verschlüsselungstechnik. Dabei wird bei jeder Position des Klartextes eine andere Substitution angewendet. Zur Verschlüsselung wird ein zwischen Sender und Empfänger vorab vereinbartes Wort, dass so genannte *Schlüsselwort*, durch mehrfache Wiederholung auf die Länge des Klartextes gebracht. Für jede Position des Klartextes hat man nun ein Paar von Buchstaben, aus dem dann mittels einer Tabelle (der Vigenère-Tabelle) ein einziger Buchstabe bestimmt wird, der zur entsprechenden Position des Chiffrats wird. Dabei gelingt es, das erste Auftreten des Buchstaben „A“ z.B. in ein „H“ umzuwandeln und das zweite Auftreten in ein „G“ usw. Durch Eliminierung von Wortgrenzen, Mischung von Alphabeten sowie Verwendung langer Schlüsselwörter kann eine besonders gute Verschlüsselung erreicht werden.