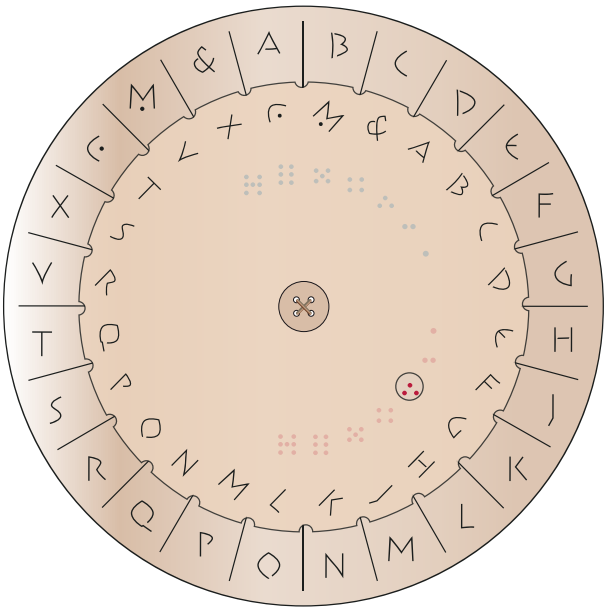
# Datenschutz auf altrömische Art



Sueton* beschreibt die Verschlüsselung
eines Geheimtextes zu Zeiten Gaius Julius Caesar's:

Zitat: *"Wenn etwas Geheimes zu überbringen war, schrieb er (J.Caesar) in Zeichen, das heißt, er ordnete die Buchstaben so, dass kein Wort gelesen werden konnte: Um diese zu lesen, tauscht man z.B den vierten Buchstaben, also D für A aus und ebenso mit den restlichen. Das Alphabet wurde rotiert je nachdem vor- oder rückwärts um die stellen die der Author bestimmte. Daraufhin wurde der Text entsprechend codiert aufgeschrieben."*

Caesar verschob angeblich gerne um 3 Positionen vorwärts A wurde zu C. Der Verschlüsselungscode wurde mit dem ersten Buchstaben im gesendeten Text angegeben der für ein A stand.

Der Code konnte auch mit dem Boten in Verbindung gebracht werden durch folgende Regel: der Wochentag an welchem der Text dem Kurier mitgegeben wurde, bzw. die Nachricht abgesandt wurde war der Verschiebungsschlüssel. (Im ersten Jahrhundert war im röm. Reich die sieben Tage Woche verbreitet). So konnte die Nachricht nur mitsamt des Kuriers entschlüsselt werden.

Natürlich ist diese Verschlüsselungsmethode - aus heutiger Sicht - nicht sehr sicher, sie erwies sich damals im militärischen Einsatz jedoch als sehr bewährt und nützlich , davon gehen wir aus denn sie war Standard und entsprechend verbreitet.

Um Texte in sinnvoll, rasch zu chiffrieren könnte es ein Werkzeug gegeben haben, welches zwei Alphabete auf zwei kreisrunden Scheiben zueinander rotieren lässt. Die Abbildung zeigt einen mögliches Hilfsmittel der damaligen Zeit als kreisrunde Cryptograf-Doppelscheibe mit dem Alphabet. Ein derartiges Instrument hat man nicht gefunden, daher geht man davon aus dass entweder das Material vielleicht aus Holz oder Leder bestand oder noch einfacher dass man zwei Papyrii-Scheiben verwendete. Es ist auch denkbar, dass das Alphabet gradlinig, einzeilig den Rand zweier „Lineale" aus Pergament geschrieben wurde, welche dann simpel zueinander verschoben wurden.

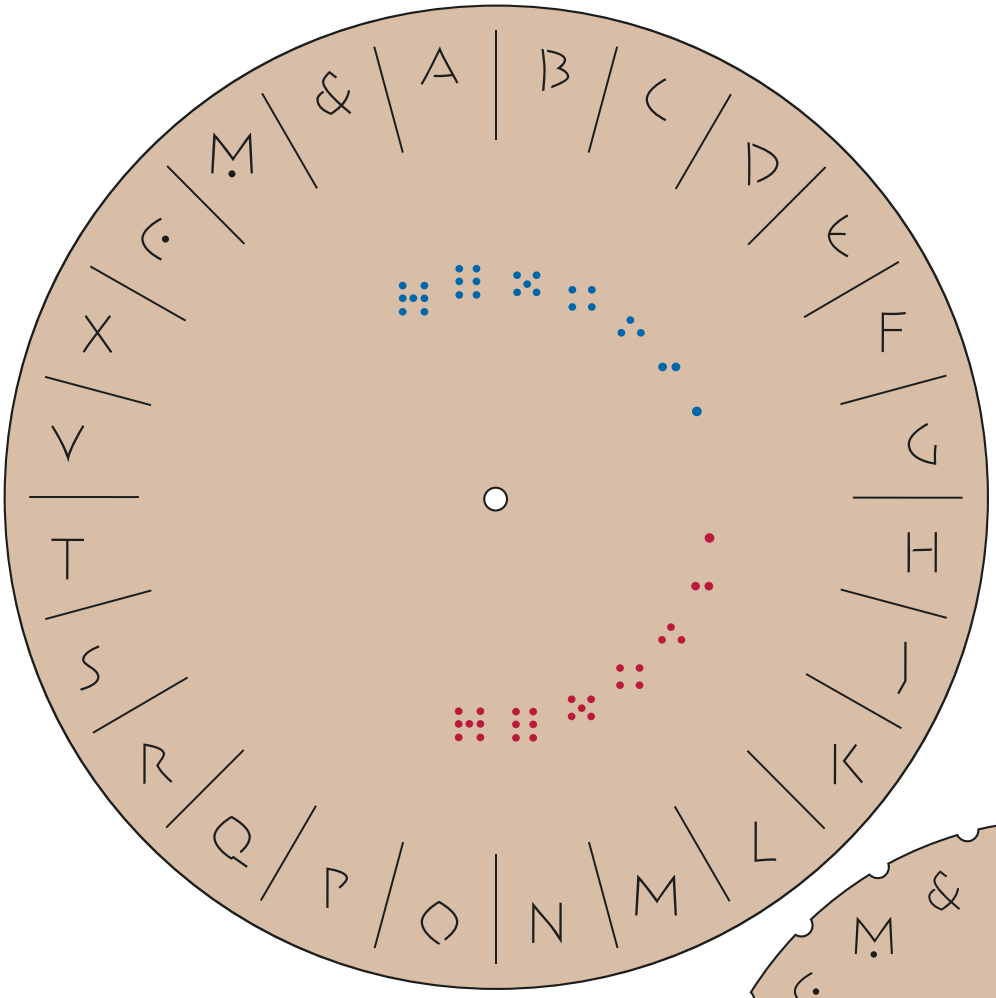
Um das Jahr 1420 hat ein italienischer Mathematiker erstmals eine passende Chiffrierscheibe dazu entwickelt. **Leon Battista Alberti's Chiffrierscheibe** erleichtert die Durchführung der Caesar-Verschlüsselung mit beliebigen Verschiebungen, indem die innere Scheibe um die Anzahl der verschobenen Buchstaben zur äußeren Scheibe gedreht wird und sich somit die ersetzten Buchstaben ablesen lassen. Darüber hinaus beschrieb Alberti auch die Verwendung der Chiffrierscheibe bzw. deren Varianten zur Durchführung von komplexeren monoalphabetischen Verschlüsselungsvarianten

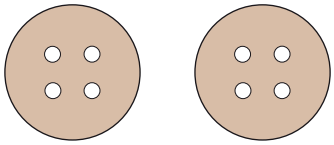
Die vorliegende **hypothetische Instrument die "antike" Chiffrierscheibe** bezieht sich auf das lateinische Alphabet im Altertum (A-X wobei U und V identisch sind und I und J ebenfalls) mit zusätzlich zwei militärisch gebräuchlichen Symbolen , nämlich c. = 100 oder auch abk. für centurie und m. = 1000 oder auch mille welches als m.m.m.m. Ode noch weiter m. Dazu für eine Legionstruppenstärke verwendet werden kann sowie das et Zeichen. Mit dieser Scheibe liegt ein Werkzeug vor mit welchem ein Kommandant schnell ver- und entschlüsseln kann sofern dies gebraucht wird.

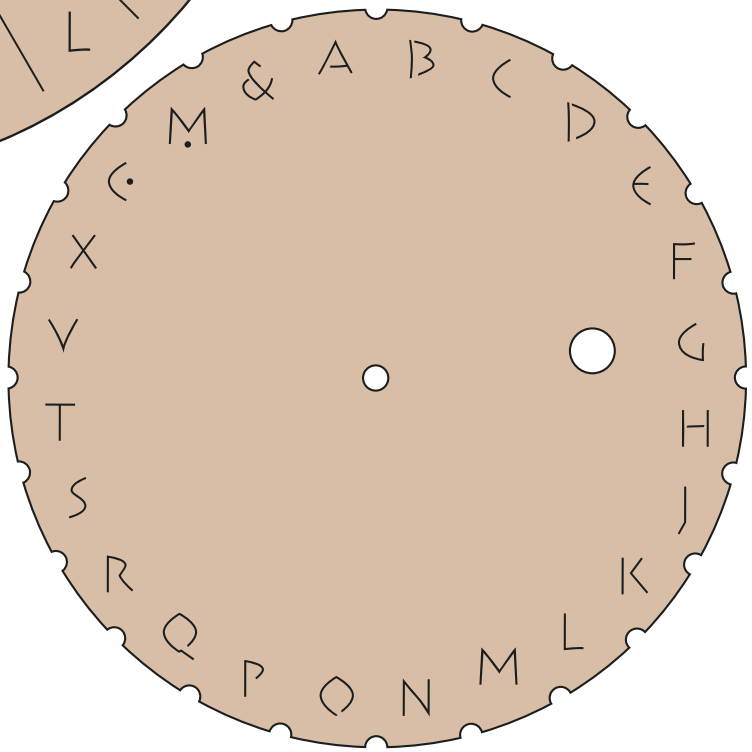
So oder sehr ähnlich wurde die Verschlüsselung vorgenommen.

*__Gaius Suetonius Tranquillus__ (deutsch Sueton; * wohl um 70; † nach 122) war ein römischer Schriftsteller und Verwaltungsbeamter und später Historiker und Biograf. Suetons bedeutendstes Werk sind die Kaiserviten (lateinisch De vita Caesarum libri VIII = Acht Bücher über das Leben der Kaiser), in denen er das Leben Caesars und der römischen Kaiser von Augustus bis Domitian schildert. Für die modernen Historiker liefert er mit seinen Schriften eine wertvolle Informationsquelle über das Leben römischer Gelehrter sowie der ersten römischen Kaiser. ( Quelle: www.vitaromana.net/praetoriani )

Kryptografie - Hypothetische römische Chiffrier-Scheibe - Modellset zum auschneiden
von www.VITA ROMANA.net






Ein weiterer Beitrag zur Informations-Sicherheit:

## Siegeltechnik für Wachstafeln

Der römische "Leseschutz" hat noch eine weitere, durch Fundstücke belegte, Komponente: zwei Wachstafeln wurden mit Leseseiten nach innen zugeklappt und miteinander verschnürt. Am Knotenpunkt ging die Schnur durch eine kleine Messing Schale in welche ein Wachssiegel des Absenders gesetzt wurde. Somit konnte der Empfänger sofort erkennen ob jemand das Siegel durchbrochen hatte und die Nachricht bereits nicht mehr als geheim betrachtet werden konnte. Das passende Siegel setzte der Absender für gewöhnlich mit seinem persönlichen Siegelring.