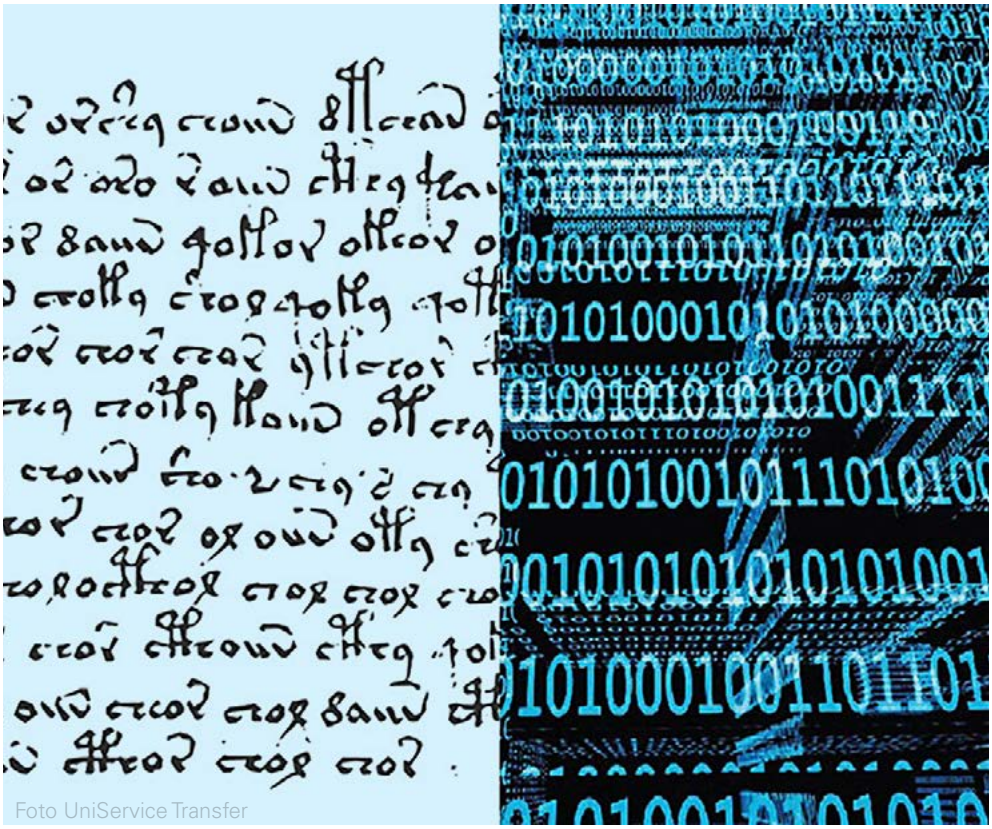

Foto UniService Transfer

Bergische Transfergeschichte

Wissenschaftliche Codeknacker

Eine interdisziplinäre Kooperation der Bergischen Universität beschäftigt sich mit modernen Dechiffrierprogrammen zur Entschlüsselung von Geheimschriften.

Kryptographie beschreibt die Wissenschaft der Verschlüsselung. Forscher*innen verschiedener Disziplinen an der Bergischen Universität arbeiten sowohl an verschlüsselten historischen Texten als auch an moderner Informationssicherheit. Gemeinsam ist allen Forschenden dabei die Entdeckung codierter Informationen und deren gleichzeitiger Schutz. In dieser interdisziplinären Kooperation finden sich erstmals Wuppertaler Historiker*innen und Informatiker*innen zusammen und stellen fest, dass sie sich gegenseitig in ihren Forschungen helfen können.

Dr. Jessika Nowak, Mitarbeiterin in der Mittelalterlichen Geschichte, stieß bei Recherchen für ihre Dissertation auf chiffrierte Gesandtschaftsberichte. „Es waren Schreiben, die gänzlich oder in Teilen chiffriert waren", sagt die Wissenschaftlerin, „in wenigen Fällen hatte man das Glück, dass

Zeitgenoss*innen schon entsprechende Entschlüsselungen vorgenommen hatten und manchmal gab es Schlüssel, die überliefert worden sind, sodass man rekonstruieren konnte, was in diesen Passagen gestanden hat.“ Meistens jedoch seien die Verschlüsselungen sehr komplex und die entsprechenden Abschnitte für Historiker*innen oft unlesbar. Der Kontakt mit den Informatikerkollegen Prof. Dr.-Ing. Tibor Jager, Dr.-Ing. Kai Gellert, Jonas von der Heyden sowie dem Leiter des Faches Digital Humanities, Prof. Dr. Patrick Sahle, eröffnete ihr dazu auf einmal neue Möglichkeiten.

Von der Kunst zur Wissenschaft

Geheimschriften gab es schon im alten Ägypten, sie wurden bis in die Gegenwart immer wieder aus politischen Gründen zu taktischen Zwecken genutzt. Viel hat sich in der Vergangenheit getan, doch der beeindruckendste Fortschritt gelang erst 1984, denn dann wurde die sogenannte beweisbare Sicherheit erfunden. „Manche Leute sagen, das war der Zeitpunkt, wo die Kunst der Verschlüsselung zur Wissenschaft der Verschlüsselung geworden ist“, sagt Prof. Dr.-Ing. Tibor Jager, Leiter der Abteilung IT-Sicherheit und Kryptographie, „seitdem können wir besonders gute und mathematisch beweisbar sichere und praktische Chiffren bauen.“

Um die Herangehensweise kryptographischer Geschichtsforschung und die Anwendung sicherer kryptographischer Verfahren der Informatik zu verstehen, bedurfte es zunächst einiger Gespräche zwischen den Wuppertaler Forschenden, in denen die sehr unterschiedlichen Fächer ihre Arbeitsweise erläutert haben. Die moderne Cryptocommunity hat nämlich einen ganz anderen Ansatz, forscht mit anderen Mitteln und auch anderer Literatur. Historisch chiffrierte Dokumente sind in den Archiven oft schwer zugänglich.

Codes automatisiert knacken

Das große Problem bei alten Stücken: Diese seien nicht digitalisiert und somit nur sehr zeitaufwendig einsehbar, weiß Tibor Jager. „An dieser Stelle wird es nun für uns Informatiker*innen interessant. Denn es stellt sich nicht so sehr die Frage, wie man das knacken kann, sondern wie man das im großen Stil automatisiert knacken kann, also ohne diese Fleißarbeit.“ Denn nun könne man, erklärt Jonas von der Heyden aus der Abteilung IT-Sicherheit und Kryptographie, „Algorithmen entwickeln, mit denen man verschlüsselte Dokumente automatisiert untersuchen und entschlüsseln kann. Dazu brauchen wir wiederum die Historiker*innen, die die Ergebnisse auf Plausibilität prüfen und auch Symbole erläutern, die man dann ins Programm eingeben kann.“

Historische Dokumente digitalisieren

An dieser Stelle kommt das dritte Fach „Digital Humanities“ unter Leitung von Prof. Dr. Patrick Sahle ins Spiel. Er fungiert sozusagen als Mittler zwischen der Geschichte und der Informatik und er weiß, wie diese historischen Dokumente in die Digitalisierung überführt werden können.

Die Aufbereitung historisch chiffrierter Dokumente für die moderne Forschung ist nach Sahles Meinung schon weitgehend standardisierte Praxis. „Schwieriger wird es aber in kleineren Archiven oder solchen, die keine eigene Digitalisierungsabteilung haben“, erklärt der Fachmann. Oft müsse man leider auf einfache Handyfotos, Fotokopien oder z. B. die Mikrofilme zurückgreifen, die es in Archiven schon gebe.

Authentizität muss gewahrt bleiben

Die kulturgeschichtliche Dimension und die Authentizität der Dokumente dürfe natürlich nicht verloren gehen, erklärt Sahle. „Für die Transparenz und Nachprüfbarkeit der Verarbeitung und Entschlüsselung würde man gerne die chiffrierten Texte auch in den Chiffren selbst wiedergeben. Einen entsprechenden Font, also eine Schriftart, zu kreieren, ist kein Hexenwerk und ‚mittel aufwendig‘.“ Da es sehr viele Chiffrierschlüssel und stark abweichende Zeichensysteme gebe, sei vor allem zu prüfen, wie weit solche Prozesse automatisiert werden könnten.

Bis es soweit ist, dass man flächendeckend alte Manuskripte in den Archiven über Computerprogramme algorithmisch auswerten kann, werden Historiker*innen wie Dr. Jessika Nowak noch lange in akribischer Fleißarbeit verschlüsselte Dokumente und Briefe über Intrigen, Liebe, Macht und Herrschaft beforschen und sich auch über kleine Entschlüsselungen riesig freuen.

UWE BLASS

Lesen Sie die gesamte Transfergeschichte **hier.**

100 TRANSFERGESCHICHTEN IN EINEM BUCH

Seit 2016 führt der UniService Transfer der Bergischen Universität Wuppertal regelmäßig Gespräche mit Wissenschaftler*innen der Uni über deren Forschungsprojekte. Mehr als 100 Transfergeschichten sind seitdem daraus entstanden. Diese sind nun in einem Sammelband erschienen. Das Buch ist beim UniService Transfer erhältlich.

Zur Buchbestellung