Historia i podstawy kryptografii
Spotkanie 4
Kryptologia w średniowieczu
Analiza częstotliwości

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Upadek kryptografii w Europie

4 września 476, dowódca germańskich najemników, pozostających w służbie Rzymu, imieniem Odoaker, obalił ostatniego cesarza Romulusa Augustulusa i wygnał go ze stolicy imperium.

Wydarzenie to przez wielu historyków uznawane jest za symboliczny koniec starożytności i początek średniowiecza
W wyniku upadku cywilizacji rzymskiej nastąpił ogólny upadek kultury i nauki, w szczególności:

- zanik umiejętności czytania i pisania

i w konsekwencji

- brak możliwości i potrzeby uprawiania kryptografii.

Upadek kryptografii w Europie

W nielicznych manuskryptach pojawiają się ślady „zabaw kryptograficznych" uprawianych przez, prawdopodobnie, znudzonych skrybów klasztornych: są to zaszyfrowane pojedyncze słowa lub zwroty, podpisy i przypisy do właściwego tekstu.

Metody szyfrowania nie grzeszyły wyrafinowaniem:

- tekst pisano od tyłu,
- stosowano szyfr Cezara z kluczem $k = 2$ (czyli *de facto* szyfr Oktawiana Augusta),
- zastępowano samogłoski kropkami,
- pisano łacińskie teksty stosując alfabet grecki lub hebrajski.

Z tysiącletniego okresu od V w. do XV w. zachowały się przekazy tylko o nielicznych osobach stosujących szyfrowanie tekstów.

Upadek kryptografii w Europie

- **św. Bonifacy**, mnich anglosaski żyjący w VIII w., rozpowszechniał w Niemczech zagadki, w których samogłoski były zastąpione kropkami,
- mnich **Gerbert**, późniejszy papież **Sylwester II** i jeden z najbardziej wykształconych ludzi X w., posługiwał się *notami tyrońskimi*, czyli rodzajem stenografii opracowanej przez Tyrona, wyzwoleńca Cycerona,
- **św. Hildegarda z Bingen**, mniszka i mistyczka z XII w., posługiwała się tajnym alfabetem, poznanym w czasie wizji,
- **Roger Bacon**, żyjący w XIII w., w dziele *Secret Work of Art and the Nullity of Magic* wyliczył siedem sposobów utajniania pisanych informacji,
- **Goeffrey Chaucer**, żyjący w XIV w. angielski poeta, dyplomata i filozof, w dziele *The Equatorie of the Planets* zamieścił sześć krótkich szyfrowanych opisów praktycznego obliczania orbit planet.

Rozkwit kryptologii w krajach arabskich

W ciągu około stu lat jakie upłynęły od śmierci Mahometa Arabowie opanowali znaczną część Afryki Północnej i Półwysep Iberyjski i stworzyli wielką cywilizację. Rozwijali literaturę i naukę, w szczególności medycynę i matematykę. Słowa *cyfra* i *szyfr* pochodzą z języka arabskiego.

Powszechna znajomość sztuki czytania i pisania, związana z koniecznością studiowania Koranu, oraz silnie rozwinięta dyplomacja spowodowała wzrost zainteresowania kryptografią.

Praca licznych arabskich uczonych zaowocowała rozwojem studiów lingwistycznych, jak również dziełami na temat szyfrowania wiadomości.

Przełomem dokonanym w świecie arabskim było odkrycie metody łamania monoalfabetycznych szyfrów podstawieniowych.

Rozkwit kryptologii w krajach arabskich

Wybitnymi uczonymi zajmującymi się teorią szyfrowania byli między innymi:

- **Abu ‘Abd ar-Rahman al-Khalil ibn Ahmad ibn ‘Amr ibn Tammam al-Farahidi al-Azdi al-Yahmadi** (718 – 786), zwany **al-Farahidi** lub **al-Khalil**. Był on autorem m.in. pierwszego, wielotomowego słownika języka arabskiego oraz (zaginionego) dzieła poświęconego kryptografii *Księga o szyfrowaniu wiadomości*, w której po raz pierwszy została zwrócona uwaga na różnice w częstotliwości pojawiania się poszczególnych liter.
- **Abu Yusuf Yaqub ibn Ishaq as-Sabbah al-Kindi**, zwany **al-Kindi** – wszechstronny uczony, który po raz pierwszy opisał w dziele *O odczytywaniu tajnych listów* metodę **analizy częstotliwości**, czyli procedury służącej do łamania monoalfabetycznych szyfrów podstawieniowych.

Czym jest analiza częstotliwości?

Uczeni arabscy opisali kolejne kroki postępowania wykonywane przy stosowaniu analizy częstotliwości:

- na podstawie **długiego** tekstu jawnego, należy ustalić częstotliwości występowania poszczególnych liter,
- należy obliczyć częstotliwości wszystkich znaków, które występują w tym tekście,
- należy rozpocząć pracę od postawienia **hipotezy**, że najczęściej występujący znak w tekście tajnym odpowiada najczęściej występującej literze,
- jeśli hipoteza ta nie daje wyniku, trzeba zastąpić najczęściej występującą literę drugą, co do częstotliwości, literą danego języka, itd
- należy zwracać uwagę na inne elementy charakterystyczne dla języka: spójniki, zbitki dwuliterowe itd.