Historia i podstawy kryptografii
Spotkanie 6
Początki epoki nowożytnej w kryptografii

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Koniec Średniowiecza

Zmiany w Europie w ostatnich dwóch wiekach Średniowiecza (wiek XIV i XV)

- powstanie silnych ośrodków władzy w wielu krajach europejskich,
- rozwój banków i handlu w Europie,
- rozwijanie sieci placówek dyplomatycznych,
- powstanie kilku ośrodków władzy kościelnej w wyniku schizmy zachodniej (1378 –1417),
- wzrost liczby ludzi wykształconych,
- przyswajanie niektórych zdobyczy cywilizacji arabskiej,
- wynalezienie druku.

Koniec Średniowiecza

Konsekwencje dla kryptologii

- konieczność stworzenia bezpiecznych sposobów przekazywania wiadomości,
- powstanie kancelarii zatrudniających wykształconych sekretarzy znających zasady szyfrowania (tzw. **tajne kancelarie**),
- odrzucenie prostych „szyfrów" średniowiecza jako nieprzydatnych (nie zapewniających bezpieczeństwa),
- zrozumienie i wykorzystywanie kryptoanalizy szyfrów monoalfabetycznych,
- poszukiwanie doskonalszych szyfrów, w szczególności odpornych na analizę częstotliwościową,
- próby „mechanizacji" procesu szyfrowania i deszyfrowania,
- możliwość publikowania wyników badań i odkryć kryptoanalitycznych.

Szyfry podstawieniowe z homofonami

Jedną z pierwszych prób przeciwdziałania analizie częstotliwości było tworzenie **szyfrów podstawieniowych z homofonami** zwanych krócej **szyframi homofonicznymi**. W szyfrach tych literom alfabetu jawnego przyporządkowywano umowne znaki (na ogół liczby dwucyfrowe), przy czym większości liter przydzielano kilka znaków zgodnie z zasadą proporcjonalności: częściej występującym literom przypisywano więcej znaków.
Początek klucza mógł więc wyglądać tak:

a	19 31 33 45 53 57 67 71 88 90
b	11 78
c	37 54 87
d	12 26 93
e	13 17 21 47 48 62 74 80 94
f	75

Nomenklatory

Innym sposobem wzmocnienia używanych szyfrów było tworzenie tzw. nomenklatorów, które początkowo były używane głównie przez dwory papieża i antypapieża do porozumiewania się z ich stronnikami.

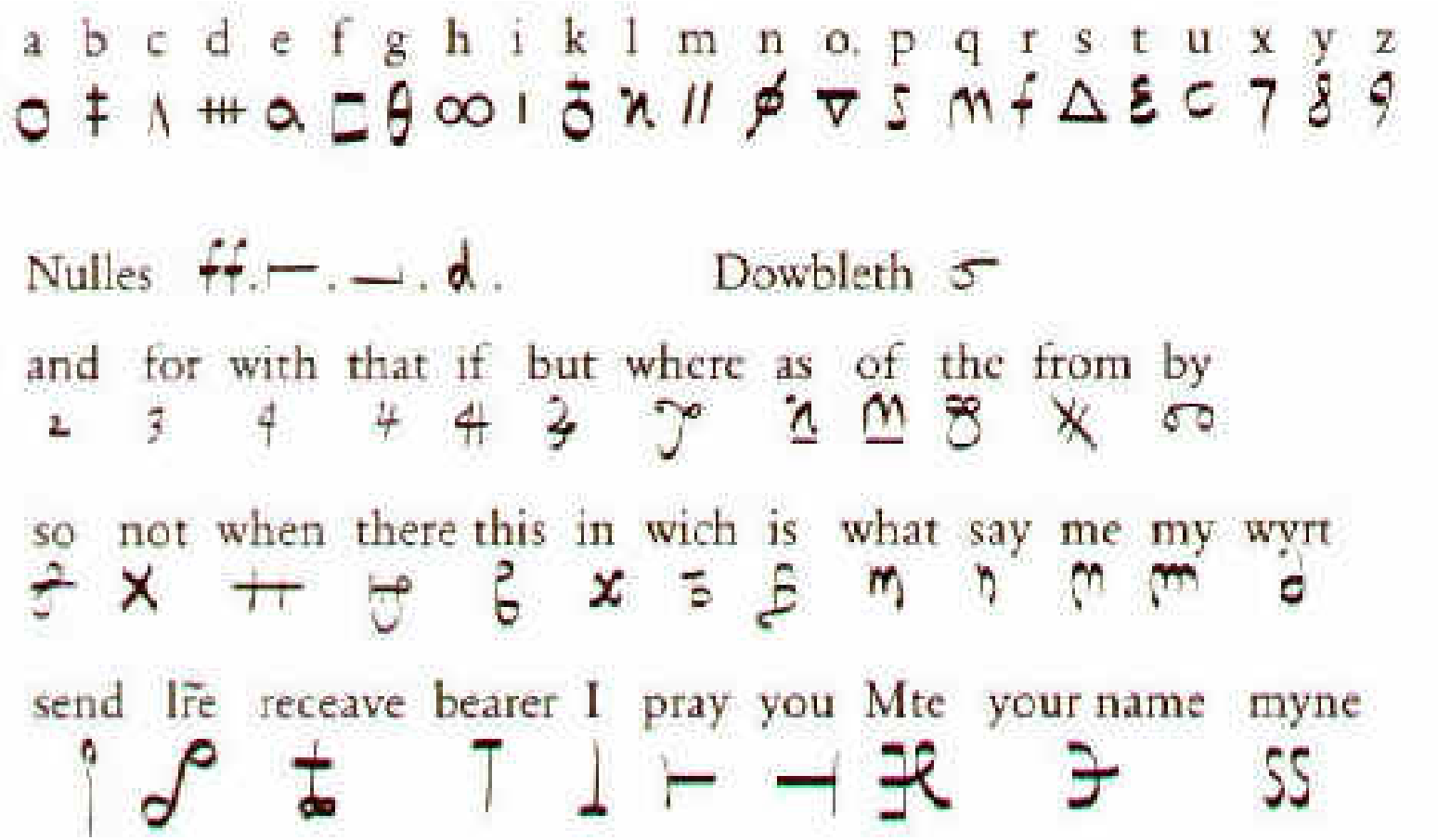
Nomenklator był kryptosystemem złożonym z dwóch elementów:

- **alfabetu szyfrowego** będącego kluczem szyfru podstawieniowego,
- **kodu**, czyli listy najczęściej wykorzystywanych sylab, słów i zwrotów, którym przyporządkowywano zamienniki w postaci kilkucyfrowych liczb lub zestawów liter.

Korzystanie z nomenklatora polegało na zastępowaniu fragmentów tekstu jawnego przez symbole kodu w każdym przypadku, gdy było to możliwe oraz korzystaniu z alfabetu szyfrowego, gdy było to konieczne.

Nomenklatory

Przykład: Nomenklator Marii Stuart (XVI w.).



Nomenklatory

Zalety nomenklatorów:

- tekst zaszyfrowany nie daje informacji o strukturze tekstu jawnego,
- kryptoanalityk widząc grupę znaków nie wie, czy ma do czynienia z literą, sylabą, słowem czy fragmentem zdania lub całym zdaniem.

Wady nomenklatorów:

- początkowo w nomenklatorach stosowano **zapis równoległy**: lista liter (sylab, słów, zwrotów) oraz lista ich zamienników były uporządkowane alfabetycznie (albo numerycznie),
- odtajnienie jednego egzemplarza nomenklatora wymuszało stworzenie nowych list i ich wymianę we wszystkich miejscach stosowania,
- nomenklatory zawierające długie listy kodów były trudne do ukrycia.

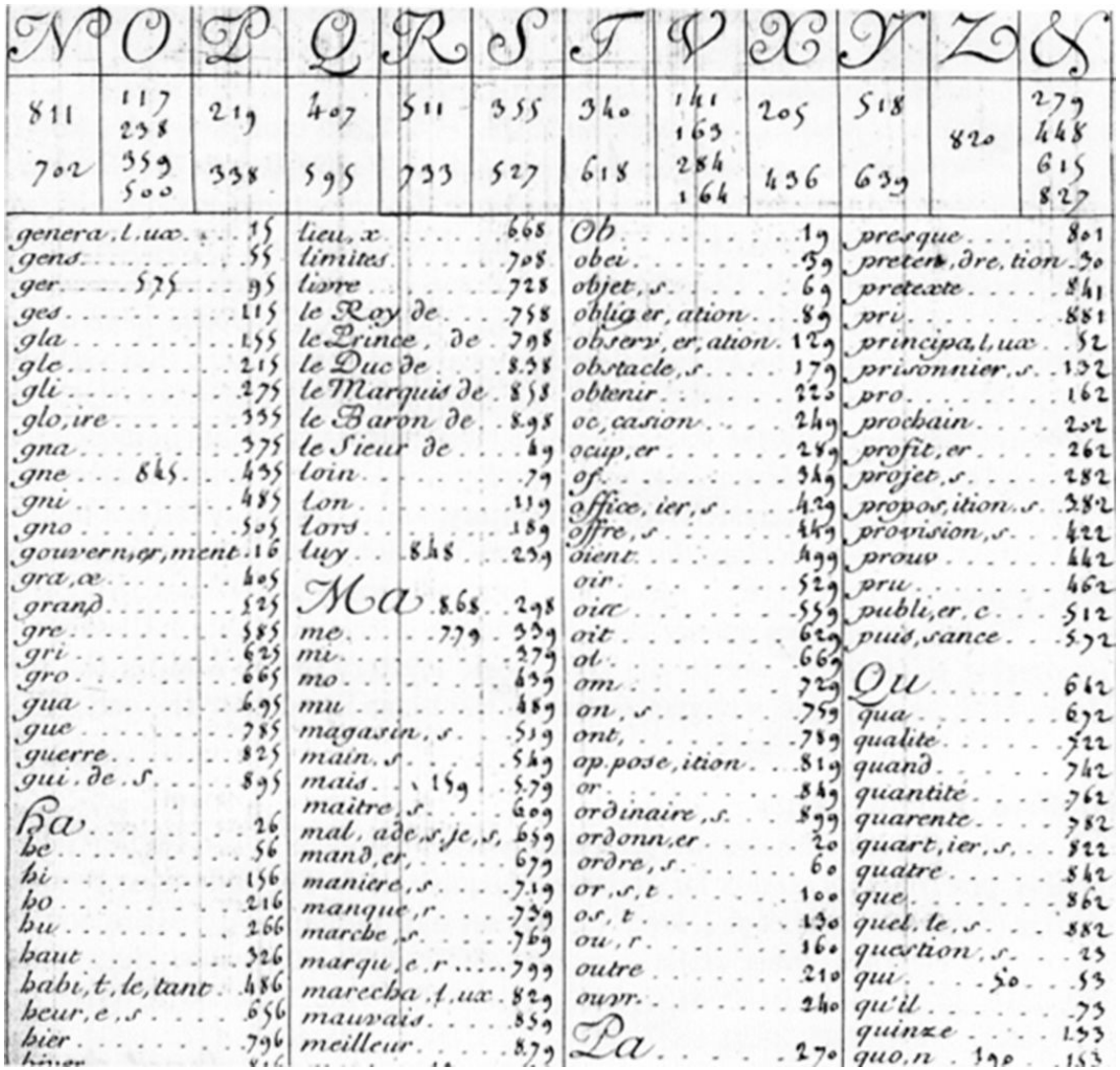
Nomenklatory

Pierwsza z powyższych wad (zapis równoległy) została usunięta przez **Antoine Rossignola** (1600 – 1682) – głównego kryptologa francuskich królów Ludwika XIII i Ludwika XIV. Rossignol wprowadził **nomenklatory dwuczęściowe**:

- pierwsza część zawierała uporządkowaną alfabetycznie listę słów i zwrotów, którym przyporządkowano losowe liczby,
- drugą część tworzyły uporządkowane numerycznie kody i ich odpowiedniki słowne.

Nomenklatory

Przykład: Stworzony przez Rossignola Wielki Szyfr – homofoniczny szyfr podstawieniowy z rozbudowanym nomenklatorem (fragment).



N	O	P	Q	R	S	T	V	X	Y	Z	&
811	117 238	219	407	511	355	340	141 163	205	518	820	279 448
702	359 500	338	595	733	527	618	284 164	436	639		615 827

genera,l,ux. 15
gens 55
ger. 575 95
ges 115
gla 155
gle 215
gli 275
glo,ire 335
gna 375
gne 845 435
gni 485
gno 505
gouvern,er,ment 16
gra,æ 605
grand 625
gre 585
gri 625
gro 665
gua 695
gue 785
guerre 825
gui,de,s 895

ha 26
he 56
hi 156
ho 216
hu 266
haut 326
habi,t,le,tant 486
heur,e,s 656
hier 796

lieu,x 668
limites 708
livre 728
le Roy de 758
le Prince, de 798
le Duc de 838
le Marquis de 858
le Baron de 898
le Sieur de 49
loin 79
lon 119
lors 189
luy 848 239

Ma 868 298
me 779 339
mi 379
mo 439
mu 489
magasin,s 539
main,s 549
mais 159 579
maitre,s 609
mal,ade,s,je,s, 659
mand,er, 679
maniere,s 719
manque,r 739
marche,s 769
marqu,e,r 799
marecha,l,ux 829
mauvais 859
meilleur 879

ob 19
obei 39
objet,s 69
oblig,er,ation 89
observ,er,ation 129
obstacle,s 179
obtenir 225
oc,casion 249
ocup,er 289
of 349
office,ier,s 429
offre,s 469
oient 499
oir 529
oire 559
oit 629
ol 669
om 729
on,s 759
ont, 789
op,pose,ition 819
or 849
ordinaire,s 899
ordonn,er 20
ordre,s 60
or,s,t 100
os,t 130
ou,r 160
outre 210
ouvr. 240

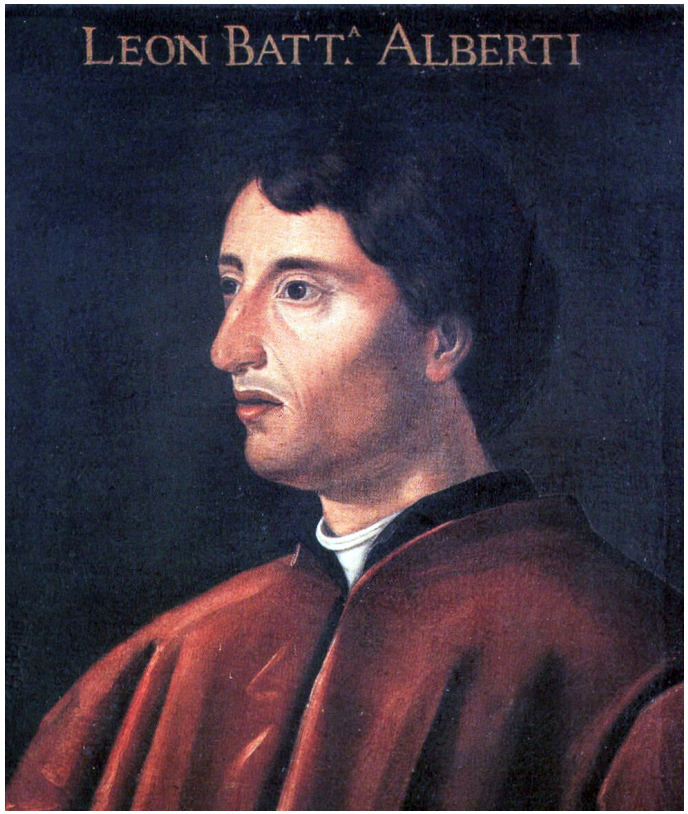
Pa 270

presque 801
preten,dre,tion 30
pretexte 841
pri 881
principa,l,ux 52
prisonnier,s 132
pro 162
prochain 202
profit,er 262
projet,s 282
propos,ition,s 382
provision,s 422
prouv 442
pru 462
publi,er,c 512
puis,sance 572

Qu 612
qua 632
qualite 722
quand 742
quantite 762
quarente 782
quart,ier,s 822
quatre 842
que 862
quel,le,s 882
question,s 23
qui 50 53
qu'il 73
quinze 133
quo,n 190 153

Leone Battista Alberti (1404 – 1472)

L. B. Alberti był pierwszym z geniuszy Odrodzenia. Wszechstronnie uzdolniony architekt, malarz, kompozytor i organista, literat i filozof.



Napisał pierwszy nowoczesny traktat o kryptologii *De Cifris* (1467).

Dysk szyfrujący Albertiego (*De cifris* 1467)

W 1467 r Leon Battista Alberti opisał pierwszą „maszynę” szyfrującą w postaci dysku zbudowanego z dwóch koncentrycznych pierścieni z umieszczonymi na nich alfabetami:

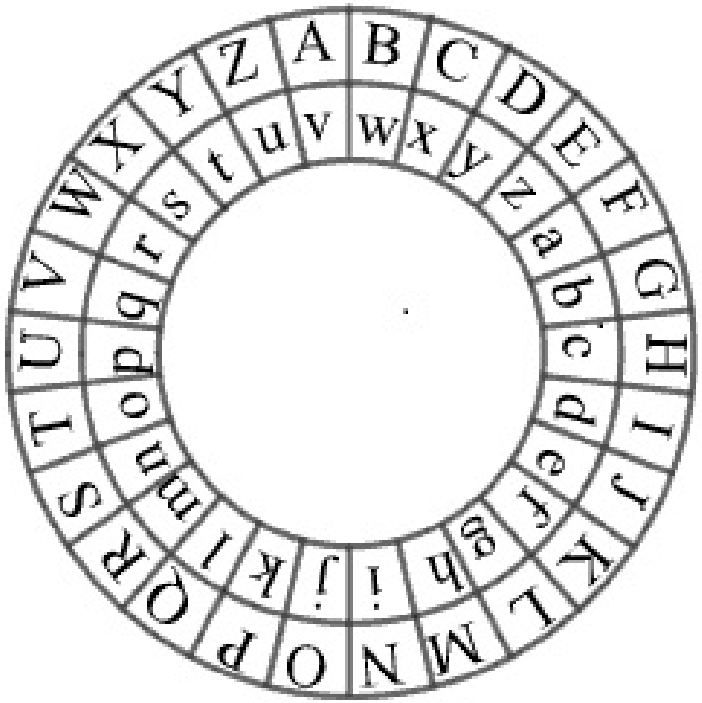
Dysk szyfrujący Albertiego (*De cifris* 1467)

Algorytm szyfrowania

- Zewnętrzny pierścień był nieruchomy, wewnętrzny obracał się wokół wspólnego środka.
- Klucz składał się z jednej litery i dwóch liczb naturalnych: **przesunięcia** $p \leqslant 4$ i **okresu** m.
- Wewnętrzny pierścień był ustawiany tak, aby ustalona litera (klucz) znalazła się pod literą A na zewnętrznym pierścieniu.
- Literom tekstu jawnego, odczytywanym na wewnętrznym pierścieniu, przypisywano litery z pierścienia zewnętrznego.
- Po zaszyfrowaniu m liter przesuwano wewnętrzny pierścień o p miejsc w prawo.

Dysk szyfrujący Albertiego

W kolejnych stuleciach używano dysku Albertiego w uproszczonej postaci, ale z pełnym 26 literowym alfabetem:



Szyfr Albertiego jest pierwszym szyfrem **polialfabetycznym**, czyli takim, w którym ta sama litera w tekście jawnym może być zaszyfrowana przez różne litery pochodzące z różnych alfabetów.