Instytut Matematyki
Uniwersytet Kazimierza Wielkiego

Kierunek: Matematyka
Specjalności:
- kryptologiczna
- finansowo-ubezpieczeniowa

Erasmus+ Matematycy aktywnie uczestniczą w programie Erasmus+. Umożliwia on naszym studentom odbycie części studiów na renomowanych uczelniach w Unii Europejskiej i nie tylko. Udział w programie Erasmus+ może być także szansą odbycia praktyki zawodowej za granicą.

Ω W Instytucie Matematyki działa Koło Naukowe Dydaktyki Informatyki i Matematyki OMEGA. Jego członkowie prowadzą zajęcia z matematyki i informatyki dla młodzieży szczególnie uzdolnionej, wdrażając opracowane przez siebie nowoczesne metody nauczania. Aktywni członkowie koła uczestniczą w studenckich i naukowych konferencjach na terenie całej Polski.

ORGANIZATORZY

Stowarzyszenie Nauczycieli
Przedmiotów Przyrodniczych i Technicznych
Skrytka pocztowa 93, 85-797 Bydgoszcz 32
tel.: 52 346 76 67, e-mail: **awjodko@wp.pl,**
www.snppit.pl

Instytut Matematyki
Uniwersytet Kazimierza Wielkiego
Pl. Weyssenhoffa 11, 85-072 Bydgoszcz
tel.: 52 341 90 01, e-mail: **imath@ukw.edu.pl**
www.ukw.edu.pl/jednostka/instytut_matematyki

Pedagogiczna Biblioteka Wojewódzka
im. Mariana Rejewskiego
W Bydgoszczy, ul. M. Skłodowskiej-Curie 4,
85-094 Bydgoszcz
tel./faks: 52 341 19 84
e-mail: **administracja@pbw.bydgoszcz.pl**
www.pbw.bydgoszcz.pl

Gość honorowy sympozjum:

Pani **Janina Sylwestrzak**

– córka Mariana Rejewskiego

UNIWERSYTET KAZIMIERZA WIELKIEGO W BYDGOSZCZY

SNPPiT

2015
Rok Matematyki
Rok Mariana Rejewskiego
(1905 – 1980)

Sympozjum

dla uczniów szkół ponadgimnazjalnych
z udziałem
Janiny Sylwestrzak

„MARIAN REJEWSKI WIELKI BYDGOSZCZANIN, MATEMATYK, KRYPTOLOG"

czyli
dlaczego warto zajmować się matematyką i kryptologią

płk Jerzy Lelwic

Marian Rejewski bydgoszczanin, matematyk, kryptolog

Plus ratio quam vis /Rozum znaczy więcej niż siła/

Marian Rejewski urodził się i wychował w Bydgoszczy, gdzie pobierał nauki w Królewskim Gimnazjum im. Fryderyka, a od roku 1920 w Państwowym Gimnazjum Klasycznym. Stąd pochodziła jego żona Irena i tu na świat przyszły ich dzieci: syn Andrzej (1936) i córka Janina (1939). Po siedmioletniej tułaczce wojennej powrócił do rodziny na ul. Dworcową 10. Przepracował 20 lat, najpierw w „Kablu", a potem w spółdzielczości rzemieślniczej. Po przejściu na rentę w roku 1967 napisał swoje wspomnienia z pracy w polskim radiowywiadzie.

Od dzieciństwa zdradzał uzdolnienia matematyczne, dlatego podjął studia na Uniwersytecie Poznańskim u prof. Zdzisława Krygowskiego. Po obronie pracy magisterskiej w roku 1929 odbył roczny staż na uniwersytecie w Getyndze, gdzie studiował metody statystyczne i matematykę ubezpieczeniową. W latach 1930–1932 był asystentem prof. Krygowskiego i jako dobrze zapowiadający się matematyk przerwał karierę naukową, aby rozpocząć przygodę z kryptologią, która zaprowadziła go na karty historii.

Zaangażowany do pracy w Biurze Szyfrów Oddziału II Sztabu Głównego, wykorzystał swoją kryptologiczną intuicję i znalazł lukę w pancerzu ochronnym niemieckiej maszyny szyfrującej Enigma. Wiedziony geniuszem matematycznym przedstawił działanie jej poszczególnych elementów jako nieznaną permutację, a ich łączne działanie jako iloczyn permutacji. Sformułował w ten sposób centralne twierdzenie kryptologii maszyn wirnikowych, tworząc teoretyczny fundament, który umożliwił skuteczne przełamanie komunikacji wroga. Równocześnie stworzył matematyczny model maszyny, który posłużył do jej zrekonstruowania. Tworząc bombę kryptologiczną, swoisty archetyp komputera, wprowadził światową kryptologię w epokę automatyzacji i wytyczył kierunek rozwoju cywilizacji cyfrowej. Alianci wykorzystali i twórczo rozwinęli pionierskie osiągnięcia Rejewskiego, a w zmaganiach z niemieckimi maszynami szyfrującymi dotarli na skraj ery informatycznej.

Pokonanie przez Rejewskiego i jego kolegów niemieckiego szyfru maszynowego oraz rekonstrukcja Enigmy należą do największych osiągnięć polskiego wywiadu. Obok wysiłku żołnierskiego, był to nasz ogromny wkład intelektualny w pokonanie państw Osi i wcześniejsze zakończenie wojny.

dr hab. Marek Wójtowicz

Ewolucja kryptologii

Szyfry dzielą się na dwie podstawowe klasy:
- symetryczne, gdy klucz szyfrujący jest jednocześnie deszyfrującym,
- asymetryczne, gdy klucze szyfrujący i deszyfrujący są różne.

Ciekawymi przykładami starożytnych szyfrów symetrycznych są te pochodzące od Juliusza Cezara, szyfry Polibiusza i Vigenere'a oraz szyfr „parkan".

Współczesne szyfry symetryczne wykorzystują mniej lub bardziej skomplikowane urządzenia szyfrujące. Należą do nich m.in.:
- tarcza Albertiego,
- Enigma,
- szyfr XOR, kodujący poszczególne bity tekstu jawnego.

Obecnie najpopularniejszym systemem szyfrującym, wykorzystywanym głównie w bankowości, jest asymetryczny kryptosystem RSA, w którym klucz szyfrujący jest *kluczem publicznym*, powszechnie znanym. Z punktu widzenia podstaw matematycznych szyfr ten jest dość prosty. Jego moc wynika z trudności obliczeniowej rozkładu dużych liczb (około 200-cyfrowych) na czynniki pierwsze.

Koło Naukowe
Dydaktyki Informatyki i Matematyki
OMEGA

Małgorzata Kędzierska
Wojciech Wątor

Szyfrowanie w praktyce

Aby w prosty sposób zakodować wiadomość, możemy każdą występującą w niej literę zastąpić inną literą alfabetu oddaloną o ustaloną liczbę pozycji. Taki sposób szyfrowania nazywamy podstawieniowym. Przykładem szyfru podstawieniowego jest szyfr Cezara. Inne metody oparte są np. na przestawianiu znaków lub ich przesunięciu.

Utajnianie informacji to zajęcie równie stare jak sama informacja. Do jednych z najstarszych użytecznych systemów kodowania należą np. grecki Skytale lub hebrajski Atbash (500 p.n.e.).

Uczestnicy warsztatów zmierzą się z tymi i innymi metodami szyfrowania, śledząc długą drogę tekstu jawnego od nadawcy, poprzez szyfrator i szyfrogram do odbiorcy i z powrotem przez deszyfrator do tekstu jawnego.

Słowniczek

Kryptologia – gałąź matematyki i informatyki dotycząca przekazywania informacji w sposób zabezpieczony przed niepowołanym dostępem

Kryptografia – gałąź kryptologii zajmująca się utajnianiem wiadomości

Kryptoanaliza – gałąź kryptologii zajmująca się przełamywaniem zabezpieczeń oraz deszyfrowaniem wiadomości