5. Historia Kryptografii

Kryptologia była używana w czasie wojen do przekazywania tajnych wiadomości. Już Spartiaci używali maszyn szyfrujących tzw. Skytale. Były to pręty, które okręcano skórą. Pisze się na niej wiadomość, od góry do dołu. Następnie odkręca się skórę. Adresat, żeby odczytać wiadomość musi mieć pręt o tej samej grubości. Dodatkowo, posłannik może założyć skórę z wiadomością jako pas, by ukryć ją dodatkowo.

Następnie, w starożytnym Rzymie powstał szyfr Cezara. Szyfr był dość bezpieczny, m. in. dlatego że ludzie którzy odkrywali wiadomości, myśleli że jest ona napisana w obcym języku. Szyfr Cezara był bardzo długo używany, dopóki nie złamali go Arabowie dzięki analizie statystycznej.

Potem, ludzie używali głównie nomenklatorów, połączenia szyfrów przestawiających litery i zamiany słów na inne.

W końcu jednak Blaise de Vigenère wymyślił swój szyfr polialfabetyczny. Szyfr Vigenere' a był uznawany za nie do złamania. W końcu szyfr ten złamał Fryderyk Kasiski w 1863 r. .

Podczas I wojny światowej niemcy używali szyfru ADFGX, dzięki którego użyciu mogli oni przeprowadzać ataki z zasadzki. Szyfr ten został jednak złamany przez Georges Painvina. Pozwoliło to francuzom na skupienie sił w miejscu, w którym niemcy chcieli zaatakować i zatrzymać ich postęp. Niemcy jednak zmienili swój szyfr na ADFGVX. Georges Painvin jednak złamał i ten szyfr. Dzięki temu francuzom udało się obronić Paryż.

W wojnie polsko-bolszewickiej bolszewicy używali głównie szyfru Cezara. Polacy mogli bardzo łatwo odczytywać te wiadomości. Polskie Biuro Szyfrów zatrudniło wtedy też pierwszych matematyków.

Podczas II wojny światowej Niemcy używali znanej Enigmy. Została ona złamana przez polskich matematyków Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego.

W 1930 r. powstała filia polskiego Biura Szyfrów, do której dołączyło osiem najlepszych absolwentów kursu kryptologii. Później filia została rozwiązana we wrześniu 1932 r. a Marian Rejewski, Jerzy Różycki i Henryk Zygalski przeszli do właściwego Biura Szyfrów. W 1938 r. Marian Rejewski zbudował bombę kryptologiczną, zbudowaną z sześciu połączonych enigm, używaną do odszyfrowywania kluczy dziennych. Henryk Zygalski stworzył zaś płachty Zygalskiego, używane do odszyfrowywania reszty wiadomości. W 1939 r. Niemcy zmienili działanie Enigmy. Polacy musieli przez to stworzyć 54 nowe bomby kryptologiczne oraz 60 płacht Zygalskiego, na co nie mieli środków. Przesłali więc dane o Enigmie Anglii i Francji. Anglicy opracowali ulepszoną wersję bomby. Dzięki temu mogli łamać szyfr Enigmy.