-C#

-.net

-.net framework

-windows forms

-enigma

Rotorový stroj – nejslavnější se nazývá Enigma. První vynalezl německý inženýr Artur Scherbius ještě během první světové války. Elektro – mechanické zařízení se skládalo z několika rotorů, které transformovaly obyčejný text na šifrovaný text, který vypadal jako úplně náhodné znaky. Enigma se stala známou hlavně ve vojenských kruzích. Německá armáda komunikovala pomocí radia, a tyto radiové vlny mohl nepřítel snadno zachytit, bylo nezbytné, aby zprávy chránili neprolomitelným šifrováním. Kompaktní a dobře přenosný stroj Enigma dobře splňoval jejich požadavky. Enigma pracovala na principu polyalfabetické šifry, libovolné písmeno se mohlo v textu objevit jako písmeno nebo i číslice. Šifrování bylo navíc prováděno pomocí tzv. krkového systému, tzn. Že při každém stisknutí kláves se rotory Emigmy posunuly o krok a změnily šifrování. Tím se vždy změnila substituční abeceda použitá na šifrování a zabezpečilo se tím, že každé písmeno bylo na jiné pozici rotoru a tím vznikla velmi impozantní a neprolomitelná šifra. Enigma také navíc obsahovala tzv. zásuvný panel nazývaný „reflektor štekerbrek“ umístěný v její přední části, což byl vlastně další rotor, který přispěl k větší kryptografické síle, protože měl biliony možných nastavení. Němci se oprávněně domnívali, že kôdy, které Enigma produkuje jsou neprolomitelné a teoreticky i jejich boj. Nepočítali však s lidskou omylností a geniálními mozky vědců. 1932 napsal matematik Maria Reijevski rovnici, která matematicky rekonstruovala zapojení rotorů Enigmy. Sice toto byl významný počin, ale bez znalosti vstupních kódů Enigmy to k ničemu nebylo. V době míru nebylo nastavení rotorů Enigmy příliš často měněno. To tedy znamenalo, že Rejewski dokázal do roku 1938 dešifrovat až 75 % zachycených zpráv. Pro zjednodušení práce, když bylo třeba zpracovat obrovské množství přichazejících informací, tým polského matematika Mariana Rejewského vytvořil stroj nazvaný BOMBA kryptologična, který dokázal najednou zpracovat až 17 tisíc možných pozic Enigmy. Tyto stroje ve své době byly velmi pokročilé, ale jejich možnost se brzy vyčerpaly. Na konci roku 1938 totiž Němci přidali ke své Enigmě další dva rotory a tím se exponenciálně zvýšili možnost různých poloh při šifrování. Polský vědecký tým tedy nutně potřeboval pomoc dalších expertů. A protože mezitím začala druhá světová válka, podělil se o své poznatky s Brity a Francouzi. Severně od Londýna v sídle Bletchley Park se soustředili významní vědci tehdejší doby jako např. Alan Turing nebo Belchmen. Do tohoto místa se poté soustředily úplně všechny získané zprávy, které dále zpracovávali kryptoanalytikové a snažili se prolomit jejich šifrovací klíč. Situace se zkomplikovala v roce 1940, protože Němci začali měnit nastavení rotoru Enigmy každý den. Pokud se tedy nepodařilo prolomit šifru do konce dne, jakýkoliv pokrok ztratil následujícího dne svůj význam. Vědec John Verywel brzy odhalil, že při nastavování rotorů nejsou Němci příliš důslední. Možná díky své lenosti je měnili proti předchozímu dni jenom nepatrně, proto bylo možné poznatky zjištěné předchozího dne využít i v den následující. To pomohlo odhalil část denního klíče. Mezitím Alan Turing pracoval na konstrukci vlastního stroje, který překonal problémy, se kterými se nedokázala vypořádat polská Bomba. Spolu s Welchmenem a jeho teoretickým poznatky o zásuvném panelu Enigmy sestrojili přístroj, který se stal začátkem úspěšného prolomení Enigmy. Vážil 1 tunu a byl vyroben v roce 1940. Dokonce druhé světové války takových přístrojů bylo vyrobeno až 220 a jejích každodenní používání vedlo k odhalení důležitých zpráv od německé armády. Ke kompletní Enigmě se spojenci dostali 9. 5. 1941, když se jim podařilo získat německou ponorku U110, kterou její vojáci opustili, aniž by zničili její zpravodajské vybavení. Vědci tak získali všechny číselníky, instrukce i seznamy klíčů k Enigmě. Získali to, aniž by o tom Němci věděli. Spojenci tak získali v druhé světové válce výhodu, kterou se jím podařilo velmi dobře maskovat a využívat ve svůj prospěch,

SANDRA. *Od CAESARA až po ENIGMU = : História šifrovania alebo KRYPTOGRAFIE = Historie šifrování nebo KRYPTOGRAFIE*. Slovensko: Dejepis Inak, 2022. online zdroj :.