Enigma@home

Projekt Enigma@Home próbuje odszyfrować 3 oryginalne wiadomości Enigmy z pomocą obliczeń rozproszonych. Dwie z nich zostały już odszyfrowane, aktualnie trwają prace nad trzecią. Sygnały zostały przechwycone na północnym Atlantyku w 1942 roku i są uważane za „nienaruszone”. Odszyfrowane wiadomości mogą wprowadzić nowe spojrzenie na pewne wydarzenia, które miały miejsce podczas II wojny światowej. Enigma@Home jest polskim projektem na platformie BOINC.

Enigma

Enigma (z gr. *Enigma* – "zagadka ") – niemiecka przenośna, elektromechaniczna maszyna szyfrująca, oparta na zasadzie obracających się wirników, opracowana przez Artura Scherbiusa, a następnie produkowana przez wytwórnię Scherbius & Ritter.

Enigma była używana komercyjnie od lat 20. XX wieku, a później została zaadaptowana przez instytucje państwowe wielu krajów. Podczas II wojny światowej maszyna ta była wykorzystywana głównie przez siły zbrojne oraz inne służby państwowe i wywiadowcze Niemiec, a także innych państw. Enigma należała do rodziny elektromechanicznych wirnikowych maszyn szyfrujących i była produkowana w wielu różnych odmianach.

Po raz pierwszy szyfrogramy zakodowane przy pomocy Enigmy udało się rozszyfrować polskim kryptologom w roku 1932. Prace Polaków, głównie Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego pozwoliły na dalsze prace nad dekodowaniem szyfrów stale unowocześnianych maszyn Enigma najpierw w Polsce, a po wybuchu wojny we Francji i Wielkiej Brytanii. W 1933 w Polsce zbudowano replikę Enigmy, co umożliwiło rutynowe deszyfrowanie niemieckich tajnych depesz.

Dane o sposobie kodowania zostały przekazane wywiadowi angielskiemu w sierpniu 1939 r. Wiedza o sposobie szyfrowania depesz niemieckich w znacznym stopniu przyczyniła się do sukcesów militarnych wojsk sprzymierzonych.

Pierwsza niemiecka depesza, kodowana przez Enigmę, została rozszyfrowana przez Polaków, w noc sylwestrową 1932 roku.

Polscy matematycy

Marian Rejewski

Henryk Zygalski

Jerzy Różycki

Kryptologia

Kryptologia (z gr. *kryptos* – "ukryty" i *logos* – "słowo") – dziedzina wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Współcześnie kryptologia jest uznawana za gałąź zarówno matematyki, jak i informatyki; ponadto jest blisko związana z teorią informacji, inżynierią oraz bezpieczeństwem komputerowym.

Zakres kryptologii obejmuje:

- utajnienie - informacji nie można odczytać bez klucza,
- uwierzytelnienie - strona wysyłająca może udowodnić swoją tożsamość,
- niezaprzeczalność - strona odbierająca może udowodnić tożsamość autora informacji,
- spójność - pewność, że informacja nie została zmieniona.

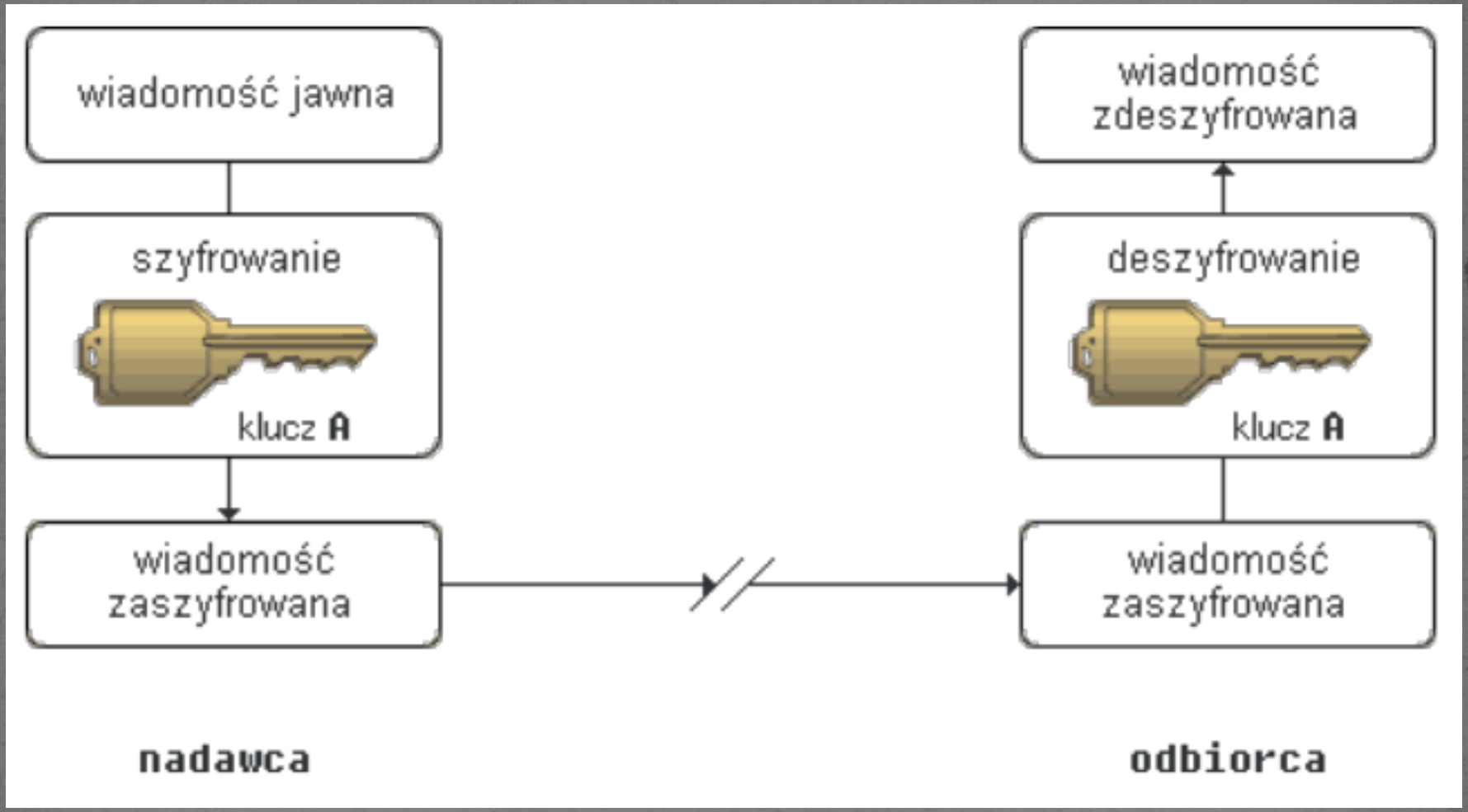
Kryptologię dzieli się na:

- **kryptografię**

(z gr. *kryptos* – "ukryty" oraz *gráfo* "pisać"), czyli gałąź wiedzy o utajnianiu wiadomości. Jest to proces przekształcania danych (tekstu jawnego) w szyfr (kryptogram, tekst zaszyfrowany) za pomocą odpowiedniego algorytmu kryptograficznego

- **kryptoanalizę**

(gr. *kryptos* – "ukryty" oraz analýein – "rozluźnić "), czyli gałąź wiedzy o przełamywaniu zabezpieczeń oraz o deszyfrowaniu wiadomości przy braku klucza lub innego wymaganego elementu schematu szyfrowania (szyfru).


wiadomość jawna
szyfrowanie
klucz A
wiadomość zaszyfrowana
wiadomość zdeszyfrowana
deszyfrowanie
klucz A
wiadomość zaszyfrowana
nadawca
odbiorca

Enigma@home

Projekt jest rozwinięciem niewielkiej, doświadczalnej sieci, złożonej z kilku domowych komputerów TJM'a - twórcy projektu. TJM testował przez parę miesięcy własne rozwiązania w zakresie użycia przetwarzania rozproszonego do łamania wiadomości zaszyfrowanych na enigmie. Kiedy zabrakło mu mocy obliczeniowej do doświadczeń, zaczął szukać pomocy u znajomych i kolegów z forum, okazało się, że zarówno część serwerowa, jak i oprogramowanie po stronie użytkowników są dość niezawodne i na odległość całość działa tak samo dobrze jak w sieci lokalnej.

Wtedy TJM uznał, że może udałoby się zintegrować jego oprogramowanie z serwerem BOINCa i tym samym wspomóc projekt **M4**.

Obecnie serwer Enigma@Home jest pośrednikiem między projektem M4 a użytkownikiem. Przenosi zadania pobrane z serwera **M4** do BOINCowego środowiska, bardziej przyjaznego użytkownikowi. Zadania pobierane są w hurtowych ilościach, dostosowywane do wymogów projektów i rozsyłane do użytkowników. Przetworzone zadania raportowane są z powrotem do oryginalnego serwera, ale wyniki przechowywane są także lokalnie, co umożliwia np. przeglądanie wszystkich rezultatów lub wygenerowanie statystyk, których brak na oryginalnym serwerze

Liczba zadań przechowywanych lokalnie, gotowych do wysłania jest zazwyczaj dość niska, ponieważ serwer automatycznie stara się utrzymywać zapas tylko na kilka godzin naprzód. Dzięki temu w bazie jest mniej rekordów i całość działa szybciej, backupy wykonywane są szybciej i zajmują mniej miejsca. Wyjątkiem są sytuacje, kiedy z góry wiadomo, że są przewidywane jakieś przerwy pobieraniu zadań, wtedy zazwyczaj buforowane jest więcej, tyle ile przypuszczalnie potrzebne będzie do momentu wznowienia normalnego działania całości. Okazjonalnie może też zadań zabraknąć, ponieważ czasami pojawiają się różne nieprzewidziane problemy.

Zadania przetworzone przez komputery użytkowników i odesłane do serwera przechodzą 3-stopniową weryfikację zanim zostaną umieszczone w bazie wyników i odesłane do serwera **M4** , żeby wykluczyć błędy które mogą powstać z rożnych przyczyn (najczęściej ze względu na problemy sprzętowe i/lub overclocking). Błędów jest jednak niezwykle mało, pojedyncze przypadki na dziesiątki tysięcy zadań. Validator projektu przyznaje stałe ilości kredytów, wyliczone dla wszystkich typów zadań na podstawie pomiarów czasu przeliczania na referencyjnej maszynie. W ten sposób liczba punktów przydzielanych za jednostkę czasu nie zależy tylko od benchmarków (które często nie odzwierciedlają prawdziwej szybkości procesora), zależy natomiast od faktycznej szybkości procesora.

Projekt ma status 'Alpha', jest stale rozwijany, często wprowadzane są w nim zmiany. Może to doprowadzić czasami do sytuacji, kiedy np. część zadań będzie wadliwa, serwer przez jakiś czas będzie nieosiągalny lub nie będzie działał poprawnie itp, jednak nie powinno to powodować żadnych większych komplikacji po stronie klienta. Jak do tej pory wszystko działa dość sprawnie i z tygodnia na tydzień eliminowane są kolejne problemy.