Zabawa kryptograficzna

Grzegorz Koperwas

3 lipca 2021

Rozwiązanie

Dla `GK` otrzymujemy `BTŚ`.

Klucz prywatny (taki bonus)

Wartość klucza prywatnego to 1057

Co ciekawe, pisząc atak (znany tekst wejściowy, znany tekst zaszyfrowany), należy sprawdzać wiele przypadków, by uniknąć potencjalnych kluczy, które mają kolizję z tym kluczem którego szukamy. Na przykład dla pary znaków `DD` występuje kolizja z pseudokluczem[1] o wartości 45.

[1] Może nie spełniać warunków