Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 390 · 2019

Informatyka i Ekonometria 15

Anna Sołtysik-Piorunkiewicz

Uniwersytet Ekonomiczny w Katowicach
Kolegium Informatyki i Komunikacji
Katedra Informatyki
anna.soltysik-piorunkiewicz@ue.katowice.pl

Patryk Niklewicz

Uniwersytet Ekonomiczny w Katowicach
patryk.niklewicz@edu.uekat.pl

METODY KRYPTOGRAFICZNE WE WSPÓŁCZESNEJ KRYPTOANALIZIE – ZAŁOŻENIA, WYZWANIA I PROBLEMY

Streszczenie: Celem artykułu jest analiza metod kryptograficznych w kontekście problemów wynikających z zapewnienia bezpieczeństwa w systemach informatycznych organizacji. Przedstawiono zmiany w podejściu do kryptoanalizy na przestrzeni lat, podstawowe założenia kryptografii jako nauki wraz z wybranymi sposobami szyfrowania danych oraz jej rolę w zapewnieniu bezpieczeństwa we współczesnym świecie. Następnie zaprezentowano przegląd metod kryptoanalizy. Biorąc pod uwagę wiele problemów związanych z zapewnieniem bezpieczeństwa systemów informatycznych, dokonano analizy wykorzystywania metod kryptograficznych oraz przedstawiono wybrane obszary, gdzie konieczne jest zestandaryzowanie metod kryptograficznych, co potwierdza także potrzebę ciągłego udoskonalania technik szyfrowania danych.

Słowa kluczowe: kryptografia, kryptoanaliza, szyfrowanie, bezpieczeństwo, poufność.

JEL Classification: L86.

Wprowadzenie

Problemy i wyzwania inżynierii bezpieczeństwa w systemach informatycznych dotyczą w dużej mierze zapewnienia poufności, integralności i dostępności, a także prywatności danych – dzięki temu możliwe staje się uzyskanie zamierzonego poziomu niezawodności systemów informatycznych. Podstawowym standardem obowiązującym obecnie w zakresie zapewnienia bezpieczeństwa w systemach informatycznych jest norma ISO. Wdrożenie norm bezpieczeństwa w organizacji pozwala na wzbudzenie zaufania partnerów i klientów biznesowych oraz spowodowanie rozwoju zrównoważonego społeczeństwa informacyj-

nego, jak również uzyskanie zmniejszenia kosztów, minimalizacji ryzyka związanego z utratą danych, a także zdiagnozowanie luk w bezpieczeństwie. Polska norma PN-ISO/IEC 27001:2017 obejmuje 14 obszarów determinujących bezpieczeństwo danych i informacji w organizacji. Skupia się ona na zagadnieniach związanych z polityką bezpieczeństwa i organizacją systemu zarządzania bezpieczeństwem pod kątem zarządzania dostępem do danych, komunikacją oraz utrzymania ciągłości działania. Ponadto norma ta precyzuje wymogi dotyczące stosowania kryptografii dla zapewnienia bezpieczeństwa informacji w systemach informatycznych i przeciwdziałania incydentom związanym ze złamaniem stosowanych algorytmów zabezpieczeń oraz utratą poufności i integralności danych ze względu na wystąpienie ataku związanego z jedną ze znanych metod kryptoanalizy.

W punkcie pierwszym artykułu przedstawiono genezę kryptoanalizy, a w drugim rozwój metod kryptograficznych na podstawie analizy dostępnej literatury przedmiotu. W trzeciej części zaprezentowano porównanie metod kryptoanalizy, które obecnie mogą stanowić zarzewie ataków cybernetycznych. W ostatnim passusie dokonano przeglądu obszarów, w których występuje konieczność zestandaryzowanego podejścia do szyfrowania danych. W podsumowaniu artykułu dokonano zestawienia wniosków na temat stosowania metod kryptograficznych i zaproponowano kierunki dalszych badań.

1. Geneza współczesnej kryptoanalizy

Kryptoanaliza stanowi jedno z wyzwań współczesnego świata dotyczących bezpieczeństwa danych w systemach informatycznych w zakresie zapewnienia poufności, integralności, dostępności informacji, a także jej autentyczności i niezaprzeczalności. Na jej cel składają się analiza i rozwój metod kryptograficznych do zabezpieczenia treści przed nieupoważnionym dostępem. W związku z rozwojem metod kryptograficznych poszukuje się coraz lepszych sposobów na zabezpieczenie treści danych z zastosowaniem kodów, szyfrów i innych sprzętowych oraz programowych metod zabezpieczeń. Jednak potrzeba zabezpieczenia informacji przed nieupoważnionym dostępem nie jest niczym nowym, gdyż proces ten sięga czasów, kiedy ludzkość umiała się komunikować na tyle dobrze i była na tyle rozwinięta w ramach obowiązujących struktur, że istniały przestrzenie i miejsca, w których informacja, przekazywana ustnie czy pisemnie, musiała być ukrywana. Najbardziej elementarnym przykładem są rozkazy wojskowe, ze względu na obecność szpiegów innych państw czy grup, które nie

sprzyjały panującej władzy. Różnica wynika ze stosowania medium służącego do przetwarzania, przesyłania i udostępniania danych, którym obecnie jest forma cyfrowa danych.

Termin „kryptoanaliza" wywodzi się z greckich słów *kryptós* „ukryte" i *analýein* „rozwiązać". Wiąże się z innym słowem greckiego pochodzenia, jakim jest „kryptografia", wywodząca się od *kryptós* „ukryte" oraz *graphein* „do zapisania". Tak jak kryptografia zajmuje się tworzeniem szyfrów i ukrywaniem pewnych informacji, tak kryptoanaliza służy do odkrycia zastosowanych metod szyfrowania i zdobywania informacji z zaszyfrowanych danych. Greckie pochodzenie tych słów również nie jest przypadkowe, gdyż już w starożytnej Grecji wraz z rozwojem matematyki rozwijały się techniki kryptograficzne. Przykładem jest spartańskie urządzenie zwane „scytale" z V w. p.n.e., będące metalowym prętem o podstawie wielokąta owijanym pasem [Karbowski, 2006, s. 19]. Nauka zajmująca się kryptografią i kryptoanalizą to kryptologia.

Proces wykorzystania szyfrów do zabezpieczenia danych rozpoczął się już kilkaset lat temu i rozwija się stale. Zgodnie z formą przetwarzania danych współcześnie rozwój metod kryptograficznych koncentruje się wokół zabezpieczenia danych cyfrowych.

2. Istota kryptografii

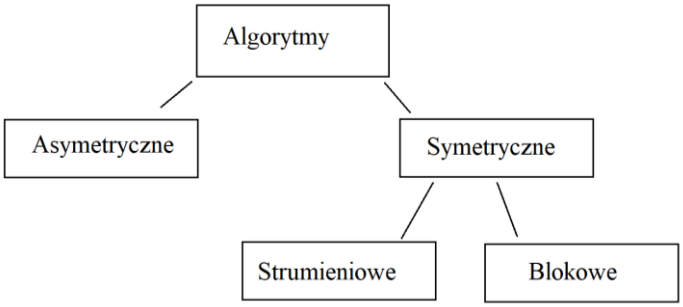
Kryptografia dotyczy tworzenia procedur zabezpieczających dostęp do danych. W praktyce polega ona na takim przekształcaniu treści przekazywanej informacji, by nie była ona możliwa do odczytania w prosty sposób. Jej podstawowym celem jest utrzymanie prywatności danych (poufności), integralności danych (utrzymanie ich jednolitości w czasie całego procesu), autentyczności (możliwość weryfikacji pochodzenia danych) oraz niezaprzeczalności (brak możliwości wyparcia się pełnionej roli przez nadawcę) [Menezes, van Oorschot, Vanstone, 1997, s. 4].

W kryptografii kluczowe są następujące pojęcia [Kutyłowski, Strothmann, 1998, s. 3]:

- tekst jawny – tekst, którego treść ma być zaszyfrowana,
- klucz – wartość, zbiór wartości lub ciąg znaków, według których szyfrowana będzie dana treść,
- kryptogram – tekst jawny zaszyfrowany za pomocą klucza.

Zgodnie z założeniami bezpieczeństwa danych poufność w systemach informatycznych jest możliwa do zapewnienia dzięki stosowaniu odpowiednich technik szyfrowania danych opartych na szyfrach podstawieniowych, przestawieniowych, macierzowych, z użyciem kluczy prywatnego i publicznego w kryp-

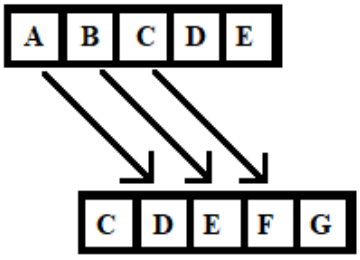
tosystemach symetrycznych lub klucza prywatnego w kryptosystemach asymetrycznych. Klasyfikację algorytmów ze względu na ich własności przedstawiono na rysunku 1.



Rys. 1. Podział algorytmów w zależności od właściwości klucza

Źródło: Opracowanie własne.

Historia kryptografii rozpoczyna się od konieczności zapewnienia poufności podczas wymiany komunikatów w społeczeństwie. Jednym z dawnych sposobów zabezpieczania danych podczas ich udostępniania było pieczętowanie kopert z listami, jednak ta praktyka pozwalała tylko na potwierdzenie, że adresat (przy właściwym doręczeniu) był pierwszą osobą czytającą list. Nie dawało to jednak żadnego zabezpieczenia w przypadku kradzieży przesyłki. Już w starożytności Juliusz Cezar opracował prosty szyfr pozwalający na kodowanie informacji. Szyfr Cezara polegał na przestawieniu każdej litery tekstu jawnego o dokładnie trzy miejsca w alfabecie, co dawało literę kryptogramu. Był to prosty szyfr podstawieniowy, jednak wystarczał w tamtych czasach do zabezpieczenia informacji. Schemat działania szyfru Cezara prezentuje rysunek 2.



Rys. 2. Przykład działania szyfru Cezara

Źródło: Opracowanie własne.

Kolejnym szyfrem utworzonym w starożytności był szyfr Atbash. Jego nazwa wzięła się z położenia liter w alfabecie hebrajskim, ponieważ jego działanie, tak jak w przypadku szyfru Cezara, opierało się na zmianie liter w zależności od

ich odległości w alfabecie, tu jednak chodziło o odległość od końca bądź początku alfabetu. I tak, pierwsza litera alfabetu hebrajskiego (alef) jest zamieniona za pomocą ostatniej litery (taw), natomiast druga litera (bet) zastąpiona zostaje literą przedostatnią (szin) i tak dalej.

Z czasem rozwój związany z postępem cywilizacyjnym pozwolił na wprowadzenie coraz lepszych metod szyfrowania, jakimi był np. szyfr Vernama, który operował już na zapisanych w postaci binarnej danych. Szyfrowanie wykonywało specjalnie stworzone w tym celu urządzenie, które w ramach działania dokonywało operacji XOR na poszczególnych bitach. W ramach udoskonalania szyfru uznano, że – aby mógł być w pełni skuteczny jako sposób zabezpieczania danych – powinien on posiadać klucze jednorazowego użytku.

Kolejnym przełomowym krokiem w historii zabezpieczania danych było zaprojektowanie maszyny Enigma, początkowo stworzonej do celów komercyjnych, która później stała się kluczowa podczas działań wojennych Trzeciej Rzeszy. Podobnie jak w szyfrze Vernama jej działanie było oparte na zastosowaniu urządzenia, które wykonywało pewną procedurę kodowania. Posiadała ona kilka wirników, przez które przepływał prąd w momencie naciśnięcia przycisku kodowania. Dzięki odpowiedniemu ustawieniu wirników pozwalała ona na szyfrowanie tekstu wejściowego za pomocą podświetlania odpowiedników naciskanej litery powyżej fizycznej klawiatury. Zaprojektowano kilka modeli Enigmy, przy czym model drugi posiadał możliwość wydruku z maszyny do pisania, natomiast trzeci zawierał lampy wskaźników [Menezes, van Oorschot, Vanstone, 1997, s. 244]. Ostatecznie jej funkcjonowanie, a w konsekwencji metoda na jej złamanie, zostało odkryte przez Polaków, co przyczyniło się zmniejszenia przewagi Trzeciej Rzeszy w trakcie II wojny światowej [Niemiec, Nowak, Grabara, 2006, s. 63].

2.1. Wybrane algorytmy szyfrujące z II połowy XX w.

Kolejny krok w rozwoju kryptografii jest związany z rozwojem informatyki, tworzeniem i zastosowaniem algorytmów szyfrowania danych, które operowały na danych binarnych. Dzięki wzrostowi mocy obliczeniowej zwiększyły się możliwości pracy na danych cyfrowych, przez co stworzono wiele algorytmów służących do szyfrowania tych danych.

Poniżej zaprezentowano i opisano wybrane algorytmy szyfrujące z drugiej połowy XX w.:

- DES,
- 3DES,

– IDEA,
– RC5,
– AES.

Jednym z algorytmów wykorzystywanych w praktyce do asymetrycznego szyfrowania danych jest RSA (algorytm R. Rivesta, A. Shamira, L. Adlemana), który do szyfrowania wykorzystuje klucze publiczny i prywatny, obliczane na podstawie danych liczb pierwszych [Chrzęszczyk, 2010, s. 154], co wpływa znacząco na bezpieczeństwo danych, ponieważ klucz publiczny jest ogólnie dostępny, a klucz prywatny nie (każdy może zaszyfrować dane, ale tylko osoby z kluczem prywatnym są w stanie je odszyfrować) [Koblitz, 2000, s. 17]. Algorytmy symetryczne w praktyce wykorzystuje się natomiast m.in. dzięki szyfrowi Vernama, opartemu o generowanie strumienia bitów klucza. Szyfr ten nazywany jest szyfrem z kluczem jednorazowym, ponieważ każde kolejne wykorzystanie wybranego klucza do szyfrowania wiadomości znacząco zwiększa ryzyko odkrycia go [Buchmann, 2001, s. 110].

Warto również wspomnieć o algorytmie symetrycznym DES (Data Encryption Standard) powstałym dzięki wzrostowi dostępnej mocy obliczeniowej w połowie lat 70. XX w. [Menezes, van Oorschot, Vanstone, 1997, s. 250] w IBM na zlecenie NIST (National Institute of Standards and Technology [www 1]), który tak jak szyfr Vernama jest symetryczny oraz tak jak szyfr Vernama opierał swoje bezpieczeństwo na tajności klucza zamiast na tajności samego algorytmu [Kutyłowski, Strothmann, 1998, s. 29]. Niestety wraz z rosnącą mocą obliczeniową niemożliwe stało się utrzymanie danych szyfrowanych za pomocą DES-a w bezpieczeństwie, ponieważ ze względu na niewielką długość klucza, z jakiego korzystał algorytm, był on narażony na ataki typu brute-force, w których atakujący sprawdza najbardziej oczywiste, a potem wszystkie możliwe kombinacje znaków w celu poznania wartości klucza. Doprowadziło to do poszukiwania lepszych sposobów na zabezpieczanie danych.

Próbą poprawienia samego algorytmu DES jest jego odmiana nazywana 3DES, która polega na nie jednym, lecz dwóch kluczach. Początkowo algorytm szyfruje tekst jawny za pomocą klucza K1, a wynik deszyfruje za pomocą klucza K2, by ostatecznie zaszyfrować efekt poprzedniej operacji za pomocą klucza K1 [Kutyłowski, Strothmann, 1998, s. 34-35]. Taka modyfikacja pozwala w prosty sposób zwiększyć złożoność obliczeniową algorytmu, co prowadzi do zwiększenia jego bezpieczeństwa.

Jednakże oprócz samych modyfikacji algorytmu DES szukano nowych sposobów na szyfrowanie danych. Jedną z koncepcji był algorytm IDEA (International Data Encryption Algorithm), który w przeciwieństwie do DES-a nie miał być wolny od ograniczeń prawnych w kwestii używania go, gdyż DES jako

standard federalny USA był chroniony prawnie. Posiadał on 128-bitowy klucz rozbijany na podklucze i dzielił tekst na 16-bitowe bloki, na których dokonywał operacji XOR, dodawania lub mnożenia modulo. W przeciwieństwie do DES-a, który na każdym kolejnym zestawie bitów przeprowadzał te same operacje we wszystkich rundach, tutaj dochodzi do przekształceń w ramach danych pochodzących z różnych bloków. Pomimo zastosowania operacji modulo i zwiększenia bitów klucza czas wykonania algorytmu nie różni się znacząco od DES-a [Kutyłowski, Strothmann, 1998, s. 40-42].

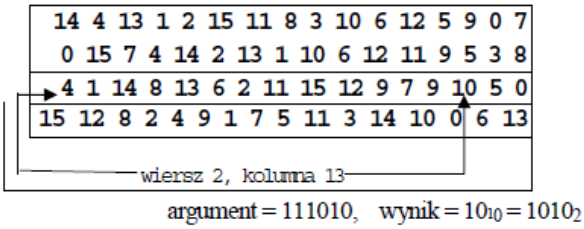
Kolejnym efektem poszukiwania nowych rozwiązań zabezpieczania danych był algorytm RC5, będący swoistą hybrydą algorytmów DES i IDEA. Jedną z najistotniejszych nowości, jakie wprowadzał ten algorytm, były parametry decydujące o liczbie wykonywanych rund (r), wielkości szyfrowanych bloków (w) czy długości klucza(b), gdzie zalecanymi wartościami są $w = 32$, $r = 12$ i $h = 16$ [Menezes, van Oorschot, Vanstone, 1997, s. 269]. W ramach działania algorytmu wykonywano dodawanie modulo, XOR ciągów określonej przez parametr długości czy przesunięcie cykliczne (zamiana pozycji bitów w danym ciągu o zadaną odległość połączona z dzieleniem modulo przez długość danego słowa). Tak jak w algorytmie IDEA dane wykorzystywane w poszczególnych rundach pochodzą z różnych bloków, nie posiada on jednak permutacji końcowej, więc dane z ostatniej rundy są danymi kryptogramu [Kutyłowski, Strothmann, 1998, s. 47].

Ostatnim wartym wspomnienia algorytmem jest AES, który tak jak DES jest symetryczny, posiada jednak 128-bitowe bloki danych oraz w zależności od wersji 128-, 196- lub 256-bitowe klucze. Zależnie od długości klucza wykonuje on odpowiednią liczbę rund (10, 12 lub 14), w ramach których na macierzach o rozmiarach 4 x 4 zwanych stanami zachodzi operacja XOR z bitami podklucza oraz operacje zamiany kolumn, wierszy lub pojedynczych bitów. Dzięki tak dużemu rozmiarowi klucza pozwala on na odpowiednie zabezpieczenie danych, co odpowiada współczesnej mocy obliczeniowej komputerów, dzięki czemu od 26 maja 2002 r. jest on standardem narodowym USA w kwestii szyfrowania danych [Bauer, 2006, s. 191].

2.2. Przedstawienie działania algorytmu DES

Algorytm DES był jednym z pierwszych algorytmów szyfrowania operującym na danych, których forma przechowywania i przekazywania była podobna do współczesnych metod zapisu danych. Wynikało to z możliwości, jakie dawała ówczesna technologia.

DES opierał swoje działanie na wykonywaniu operacji na bitach podkluczy generowanych z klucza głównego, który składał się z 64 bitów, co odpowiada 8 literom ASCII, gdzie ostatnie 8 bitów było bitami kontrolnymi (tzw. bity parzystości) [Kutyłowski, Strothmann, 1998, s. 29], oraz s-boksów, czyli macierzy zawierających 64-bitowe bloki znaków tekstu jawnego. Po wstępnej permutacji, czyli przekształceniu danych tekstu jawnego na ich dokładne odwzorowanie, gdzie każda wartość zmienia się w inną i nie może zdarzyć się tak, że dwie różne wartości po permutacji będą takie same [Aumasson, 2018, s. 5], dane w s-boksach są przetwarzane przez określoną liczbę rund. Algorytm ten w wersji standardowej wykonywał 16 rund obliczeń. W ramach każdej rundy algorytm na podstawie danych wejściowych określał dane wyjściowe wynikające w położenia ich w konkretnym s-boksie. Po wykonaniu ostatniej rundy dochodzi do ponownej permutacji, dzięki której otrzymuje się kryptogram [Kutyłowski, Strothmann, 1998, s. 29-31]. Przykład takiego s-boksa prezentuje rysunek 3.



Rys. 3. Przykład działania s-boksa w algorytmie DES

Źródło: Kutyłowski, Strothmann, [1998, s. 23].

3. Analiza podejść we współczesnej kryptoanalizie – wyzwania i problemy

Kryptoanalizę można opisać jako analizę metod szyfrowania stosowanych w zabezpieczeniu danych systemu informatycznego, której celem jest wykrycie słabych elementów zabezpieczeń. Kryptoanaliza służy uzyskaniu jak największej ilości informacji o tekście jawnym czy kluczu służącym do szyfrowania tego tekstu. Współcześnie można podzielić podejścia w kryptoanalizie na cztery kategorie, zależne od posiadanych przez nas informacji:

– *ciphertext-only*,
– *known plaintext*,
– *chosen plaintext*,
– *chosen ciphertext*.

Pierwszym typem kryptoanalizy jest podejście *ciphertext-only*, w którym znany jest kryptogram, a nieznany tekst jawny. Przykładem takiej operacji są przejmowane w czasie II wojny światowej rozkazy nadawane przez niemieckich oficerów i przejmowane przez wojska sprzymierzone, gdzie znana była treść kryptogramu, nieznane natomiast było ułożenie wirników oraz treść tekstu jawnego.

Kolejny typ kryptoanalizy to *known plaintext*, w którym znane są tylko wybrane pary: tekst jawny – kryptogram, jak ma to miejsce w przypadku zdobycia części korespondencji osób porozumiewających się szyfrem, te pary jednak nie zawsze pozwalają na odkrycie klucza, którego znalezienie jest najistotniejszą częścią kryptoanalizy.

Inny typ kryptoanalizy stanowi *chosen plaintext*, w ramach którego znany jest kryptogram dla dowolnego tekstu jawnego, ale poszukuje się klucza. Taki rodzaj analizy może wystąpić w przypadku, kiedy jest dostęp do narzędzia czy urządzenia szyfrującego, co pozwala tworzyć dowolne pary: tekst jawny – kryptogram, jednak nie daje informacji o kluczu. Wtedy należy ustalić odpowiednią liczbę par: tekst jawny – kryptogram, by móc złamać szyfr i poznać klucz.

Ostatnim analizowanym typem kryptoanalizy jest *chosen ciphertext*, w którym znane są teksty jawne dla dowolnego kryptogramu, jednakże nieznany pozostaje klucz. Taka sytuacja ma miejsce wtedy, kiedy istnieje możliwość deszyfrowania kryptogramów. Analiza tego typu jest trudniejsza niż *chosen plaintext*, pomimo tego, że wydają się bardzo podobne. Kluczowa różnica polega na tym, że w przypadku *chosen ciphertext* teoretycznie można wprowadzać dowolne łańcuchy znaków pozwalające nam dostrzec, jak przebiega proces deszyfrowania kryptogramów, jednak w praktyce coraz więcej szyfrów opiera kolejne etapy szyfrowania na wyniku szyfrowania etapu poprzedniego, co prowadzi do utrudnienia zdobycia klucza w ramach ataku *chosen ciphertext* [Kutyłowski, Strothmann, 1998, s. 29].

W zależności od dostępności zasobów, które mogą przyczynić się do włamania do systemu i zdobycia klucza, wykorzystuje się różnego rodzaju techniki i metody. Jedną z takich metod jest analiza różnicowa. Jej podstawowe założenie opiera się na analizie różnic pomiędzy danymi wejściowymi a wyjściowymi poszczególnych rund wybranych algorytmów. Współcześnie bowiem niemożliwe staje się zachowanie odpowiednich standardów bezpieczeństwa przy wykorzystaniu algorytmu, który wykonuje się tylko raz. W takim przypadku wystarczy nieraz zwykła analiza częstości, jak np. w szyfrze Cezara. Przez to algorytmy szyfrujące składają się z wielu rund, przy czym każda runda pracuje albo na wybranym wycinku danych tekstu jawnego, albo na przetworzonym już tekście jawnym. W przypadku DES-a natomiast kryptoanaliza różnicowa bada różnice

między wartościami wprowadzonymi do konkretnego s-boksa a wartościami, jakie ten s-boks wypuszcza w ramach jednej rundy. Technika ta opiera się na założeniu, że jeśli X i Y są parą wchodzących do s-boksa bitów, a różnicę między nimi można wyrazić za pomocą X XOR Y, to stosując operację XOR na bitach klucza (K), otrzymuje się X XOR K i Y XOR K, które są danymi wejściowymi dla s-boksów. Dodatkowo dzięki przekształceniom uzyskuje się (X XOR K) XOR (Y XOR K) = X XOR Y, co pozwala określić, że różnica między bitami wyjściowymi z danego s-boksa powinna być równa różnicy między danymi wchodzącymi do tego s-boksa. Dzięki takiej analizie, przy założeniu odpowiedniej różnicy w wartościach bitów, za pomocą kilku prób możliwe jest określenie najbardziej prawdopodobnych bitów klucza, a znając bity klucza, możliwe staje się odkrycie treści wszystkich zaszyfrowanych wiadomości.

4. Przykłady zestandaryzowanych obszarów zastosowania metod kryptograficznych

Obecnie stosowanie szyfrowania danych jest jedną z istotniejszych metod zabezpieczeń w systemach informatycznych. Współcześnie gospodarka opiera się na informacji i wiedzy, które stają się najcenniejszym zasobem w przedsiębiorstwach i państwach, stąd też kluczowe jest stosowanie odpowiednich zabezpieczeń systemów informatycznych. Szyfrowanie obejmuje coraz to nowsze obszary, od przesyłania danych między urządzeniami, poprzez bankowość, po kwestie bezpieczeństwa państwa. Przez mnogość urządzeń komputerowych w naszym otoczeniu użytkownicy urządzeń stwarzają ryzyko, ponieważ każde urządzenie jest potencjalną furtką dla złodzieja, który może chcieć wyłudzić dane. Jeden z przykładów obszarów, w których szyfrowanie danych jest współcześnie objęte standardem, to sieci WiFi, które coraz częściej stają się przestrzenią ataków na telefony czy inne urządzenia mobilne. W przypadku WiFi plan działania jest następujący: wystarczy włamać się do urządzenia, które udostępnia sieć, dzięki czemu zyskuje się dostęp do wszystkich danych, które w tej sieci istnieją.

Próbą zapobieżenia tego typu atakom był zatwierdzony w 2004 r. standard WiFi 802.11i, który zastąpił poprzednie rozwiązanie dotyczące bezpieczeństwa (WEP – Wired Equivalent Privacy) za pomocą WPA2 (WiFi Protected Access). Protokół WEP zakładał m.in. używanie 64-bitowego, ustawianego manualnie klucza do szyfrowania danych. WPA i WPA2 natomiast posiadał 128-bitowy, generowany dynamicznie klucz, ponadto do szyfrowania wykorzystywał także

EAP, TKIP i MIC [Chaładyniak, 2005, s. 96]. Z czasem, ponownie dzięki wzrostowi mocy obliczeniowej, zaistniała potrzeba poprawienia zabezpieczeń sieci WiFi, dlatego WPA został wyparty przez WPA2, a WPA2 z czasem wyprze ogłoszone już w 2018 r. WPA3 bazujące na 192-bitowym kluczu. Dane dotyczące standardów zabezpieczeń sieci bezprzewodowych prezentuje tabela 1.

Tabela 1. Zestawienie standardów bezpieczeństwa sieci bezprzewodowych

	WEP	**WPA**	**WPA2**	**WPA3**
Wersja standardu IEEE	802.11	Brak	802.11i	Obecnie brak
Sposób generowania klucza	Manualny	Automatyczny	Automatyczny	Automatyczny
Algorytm generowania klucza	RC4	RC4	AES	AES
Rozmiar klucza	64 bity	128 bitów	128 bitów	192 bity

Źródło: Opracowanie własne.

Inny przykład działań, w których pożądane jest zabezpieczanie przesyłanych danych, stanowi komunikowanie się drogą elektroniczną z instytucjami takimi jak banki, ubezpieczalnie czy organy państwa. W przypadku kontaktu elektronicznego ważne jest, by instytucja miała pewność odnośnie do tożsamości osoby wykonującej daną operację. Współcześnie jednak stosowanie metod autoryzacji opartej na parze login i hasło nie wystarcza, ponieważ hakerzy potrafią wykorzystać metody socjotechniczne i zmanipulować użytkowników systemów informatycznych w celu wyłudzenia tych danych, stosując tzw. phishing lub inne formy ataków cybernetycznych. W takim przypadku wskazanym rozwiązaniem są podpisy cyfrowe wykorzystujące algorytmy asymetryczne, a także stosowanie dodatkowych urządzeń, np. w formie tokenu czy innego fizycznego urządzenia podłączanego do komputera. Token wykorzystywany w transakcjach bankowych zawiera unikalny identyfikator, który strona banku odczytuje, co z kolei pozwala na weryfikację tożsamości klienta. Pozwala to też na zapewnienie bezpieczeństwa samej instytucji, ponieważ dane na tokenie są zaszyfrowane tak, by był w stanie je odczytać algorytm na serwerze banku, więc bez włamania na serwer i zdobycia informacji o odszyfrowanym tekście haker nie będzie w stanie podszyć się pod klienta danej instytucji.

Przykładem wykorzystania podpisu elektronicznego jest funkcjonujący w Polsce serwis Profil Zaufany, który umożliwia uzyskanie potwierdzenia tożsamości w postaci osobistego profilu zaufanego każdemu obywatelowi w celu realizacji spraw urzędowych online. Profil zaufany można uzyskać za pomocą wniosku złożonego w dowolnej jednostce instytucji administracji publicznej lub w wybranym banku czy innej instytucji mogącej potwierdzić tożsamość danej osoby. Dzięki temu można uzyskać dostęp do elektronicznych usług administracyjnych

potwierdzając swoją tożsamość online, jak np. gotowe rozliczenia podatkowe. Założony profil zaufany pozostaje ważny przez trzy lata, jednak po tym okresie można go przedłużyć. Obecnie[1] profil zaufany ułatwia dostęp do takich portali jak Elektroniczna Platforma Usług Administracji Publicznej, Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, Centralna Ewidencja Działalności Gospodarczej, Krajowy Rejestr Karny, Krajowa Informacja Podatkowa, a także do serwisów obywatel.gov.pl, biznes.gov.pl czy Emp@tia. W związku z rosnącym stopniem integracji państwowych systemów informatycznych profil zaufany pozwala także ubiegać się o Europejską Kartę Ubezpieczenia Zdrowotnego, przydatną w razie wyjazdu do krajów Unii Europejskiej. Profil zaufany pozwala także na wyrobienie bezterminowego e-dowodu osobistego [Bednarz, 2019]. Dodatkowo uwierzytelnienie przez profil zaufany osoby ubezpieczonej w Narodowym Funduszu Zdrowia pozwala na wykorzystanie funkcjonalności Internetowego Konta Pacjenta, bezpłatnej aplikacji dostępnej pod adresem pacjent.gov.pl [*Polacy dowiedzą się…*, b.r.] w systemie opieki zdrowotnej Ministerstwa Zdrowia pozwalającego na dostęp do danych związanych z zarządzaniem wiedzą o pacjencie [Sołtysik-Piorunkiewicz, 2018, s. 85-86], który wdrażany jest od kilku lat w Polsce i ma na celu usprawnienie zarządzania systemem opieki zdrowotnej i integrację danych o pacjencie. Obejmuje aktualnie informacje dotyczące m.in. elektronicznej recepty (system e-Recepta), elektronicznego zwolnienia (system e-Zwolnienie), elektronicznego skierowania (system e-Skierowanie) oraz innych usług świadczonych przez podmioty lecznicze [www 2].

Podsumowanie

Funkcje i algorytmy metod kryptograficznych są znane i powszechnie stosowane w zabezpieczeniu danych w systemach informatycznych organizacji. Rozwój kryptografii niesie ze sobą szansę dla zapewnienia bezpieczeństwa systemów informatycznych. Stosowanie algorytmów szyfrowania daje możliwość uzyskania poczucia zaufania do organizacji przez użytkowników systemów informatycznych. Zgodnie z analizą metod kryptoanalizy można zauważyć, iż trudne jest całkowite wyeliminowanie zagrożeń związanych z atakiem cybernetycznym na dane w systemach informatycznych, w szczególności w obszarze stosowania systemów informatycznych w Internecie z wykorzystaniem np. sieci bezprzewodowych do realizacji transakcji m.in. w handlu elektronicznym, e-administracji i innych obszarach usług elektronicznych. Przeprowadzona w ramach artykułu

[1] Stan na czas wydania niniejszej publikacji.

analiza literatury przedmiotu pozwala na określenie kierunku, w jakim zmierza współczesna kryptografia oraz zagadnień, które będą w jej ramach rozwijane. Jak można dostrzec, analizując dotychczasowy rozwój metod kryptograficznych, w najbliższym czasie metody kryptograficzne będą opierać swoją siłę nadal na zagadnieniach dotyczących teorii liczb (jak algorytm RSA wykorzystujący liczby pierwsze) oraz na długości klucza zabezpieczającego dane (jak w przypadku WPA2). Rozwój zastosowania metod szyfrowania i standardów WPA dla potrzeb komunikacji bezprzewodowej w systemach mobilnej bankowości internetowej, płatności internetowej oraz obiegu dokumentów elektronicznych w ochronie zdrowia i administracji publicznej może stanowić kolejny obszar badań. Niniejszy artykuł może być również punktem wyjścia do badań mających na celu porównanie wydajności działania wybranego współczesnego algorytmu z algorytmem DES przedstawionym w artykule.

Literatura

Aumasson J.P. (2018), *Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania*, WN PWN, Warszawa.

Bauer F.L. (2006), *Decrypted Secrets: Methods and Maxims of Cryptology*, Springer-Verlag, Leipzig.

Bednarz E. (2019), *Coraz więcej spraw załatwimy bez biegania po urzędach*, https://pieniadze.rp.pl/oszczednosci/konta-bankowe/19722-profil-zaufany-banki/ (dostęp: 31.12.2019).

Buchmann J.A. (2001), *Introduction to Cryptography*, Springer-Verlag, New York.

Chaładyniak D. (2005), *Wybrane technologie bezprzewodowej transmisji danych*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", z. 5, s. 87-101.

Chrzęszczyk A. (2010), *Algorytmy teorii liczb i kryptografii w przykładach*, BTC, Legionowo.

Karbowski M. (2006), *Podstawy kryptografii*, Helion, Gliwice.

Koblitz N. (2000), *Algebraiczne aspekty kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa.

Kutyłowski M., Strothmann W.-B. (1998), *Kryptografia – teoria i praktyka zabezpieczania systemów komputerowych*, Lupus, Warszawa.

Menezes A.J., Oorschot P.C. van, Vanstone S.A. (1997), *Handbook of Applied Cryptography*, CRC Press, Boca Raton.

Niemiec A., Nowak J.S., Grabara J.K. (2006), *Bezpieczeństwo systemów informatycznych*, Polskie Towarzystwo Informatyczne Oddział Górnośląski, Katowice.

Polacy dowiedzą się o Internetowym Koncie Pacjenta i jak radzić sobie z „niesfornymi" receptami, CSIOZ, https://www.csioz.gov.pl/aktualnosci/szczegoly/polacy-dowiedza-sie-o-internetowym-koncie-pacjenta-i-jak-radzic-sobie-z-niesfornymi-recepta/ (dostęp: 10.04.2020).

Sołtysik-Piorunkiewicz A. (2018), *Modele oceny użyteczności i akceptacji mobilnych systemów zarządzania wiedzą o zdrowiu*, Uniwersytet Ekonomiczny w Katowicach, Katowice.

[www 1] https://www.nist.gov/ (dostęp: 2.12.2019).

[www 2] https://www.csioz.gov.pl/ (dostęp: 10.04.2020).

OVERVIEW OF CRYPTOGRAPHIC METHODS FOR CONTEMPORARY CRYPTANALYSIS – ASSUMPTIONS, CHALLENGES AND PROBLEMS

Summary: The purpose of the article is to analyze cryptographic methods in the context of problems arising from ensuring security in the organization's information systems. The article presents the path that cryptanalysis has taken over the years, basic assumptions of cryptography as a science altogether with data encryption methods, and its role in the modern world. Then, an overview of cryptanalysis methods was presented. Due to the multiple problems in ensuring the security of IT systems, the use of cryptographic methods was analyzed, together with the presentation of the most important areas, where it is necessary to standardize cryptographic methods, which also confirms the need for continuous improvement of data encryption techniques.

Keywords: cryptography, cryptanalysis, encryption, security, confidentiality.