Wydawnictwo Cyfrowe poswojsku.pl

Gołębiowski Dariusz

SZYFROWANIE BEZPIECZEŃSTWO KRYPTOGRAFIA

Część 1

Podstawowe pojęcia i koncepcje

Pamiętaj proszę:
napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem i opracowaniem powieści książki pt. SZYFROWANIE BEZPIECZEŃSTWO KRYPTOGRAFIA: CZĘŚĆ 1 Podstawowe pojęcia i koncepcje.

Autorzy oraz Wydawnictwo poswojsku.pl

1. dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponoszą żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

Wydawnictwo poswojsku.pl – kontakt:
www.poswojsku.pl, bok@poswojsku.pl
ul. Paprocka 86, 98-220 Zduńska Wola
ISBN: 978-83-68360-02-8

SPIS TREŚCI

MODUŁ 2: TYPY SZYFROWANIA - str. 81

1. SZYFROWANIE SYMETRYCZNE: PODSTAWY I PRZYKŁADY (AES, DES).
    - Szyfrowanie symetryczne – co to takiego?
    - Szyfrowanie symetryczne - jak to działa?
    - Przykłady symetrycznego szyfrowania

2. SZYFROWANIE ASYMETRYCZNE: KLUCZ PUBLICZNY I KLUCZ PRYWATNY
    - Czym jest szyfrowanie asymetryczne?
    - Szyfrowanie asymetryczne - przykłady
    - Dlaczego szyfrowanie asymetryczne jest takie ważne?
    - Nieco kryptografii - podpis cyfrowy

3. OMÓWIENIE PODSTAWOWYCH RÓŻNIC ORAZ ZASTOSOWAŃ OBU TYPÓW SZYFROWANIA
    - Podstawowa różnica: Klucze
    - Szybkość działania
    - Przekazywanie kluczy
    - Zastosowanie w praktyce
    - Bezpieczeństwo
    - Wnioski: Kiedy używać którego?
    - Podsumowanie: Szyfrowanie symetryczne vs asymetryczne – kto wygrywa?
4. ODNIESIENIE SZYFROWANIA SYMETRYCZNEGO I ASYMETRYCZNEGO DO POPULARNYCH TECHNOLOGII
    - Wprowadzenie do rodzajów zastosowania
    - eDoręczenia
    - Klucze kryptograficzne na USB (np. Certum, YubiKey)
    - Bankowość elektroniczna i płatności online

WPROWADZENIE

1. SZYFROWANIE – TWOJE SUPERMOCE W CYFROWYM ŚWIECIE

Miła Czytelniczko, Drogi Czytelniku,

Wyobraź sobie ten wspaniały świat bez jakichkolwiek zamków czy innych zabezpieczeń w drzwiach. Chodzisz do pracy, wracasz do domu, a Twoje rzeczy są tam, gdzie je zostawiłeś/aś - do czasu, aż ... ktoś postanowi zajrzeć i „pożyczyć ;)” coś od Ciebie - bez Twojej zgody czy nawet wiedzy. Jak Tobie podoba się taka wizja? Chyba niespecjalnie? Prawda? A teraz zerknijmy z tego samego punktu widzenia do cyber świata.

W cyfrowym świecie tak właśnie wygląda codzienna rzeczywistość bez szyfrowania. Twoje dane są jak otwarte książki, gotowe do przeglądania przez każdego, kto ma na to ochotę. Albo jak wolisz - jak Twój dom bez jakichkolwiek antykradzieżowych zabezpieczeń. Tak! Właścicielu/ko firmy. Ciebie oraz Twojego biznesu to także dotyczy. Ty także - kolokwialnie mówiąc: "dajesz ciała" ;)!

Na szczęście jest na opisane problemy rozwiązanie! Całkiem łatwe i znane od stuleci Szyfrowanie! Tak - dokładnie tak!

SZYFROWANIE to Twoja cyfrowa tarcza - supermoc,

która pozwala chronić najcenniejsze dane przed złodziejami, wścibskimi spojrzeniami czy nawet ... własnym roztargnieniem.

Ale trzeba także pamiętać, że szyfrowanie to tylko element potężnej dziedziny wiedzy, nauki i technologii jaką jest kryptografia. W początkowych modułach tej serii będę głównie posługiwał się pojęciem szyfrowania. To na tym elemencie będziemy się skupiali. Jednakże powoli będziemy także sięgali także nieco głębiej - do kryptografii.

Ale spokojnie - nie obawiaj się. Wejście w świat kryptografii zrobimy wspólnie - krok po kroku i czasami nawet nie zauważysz, a już będziesz w obszarze kryptografii. A poza tym ona wcale nie jest aż tak straszna jak by wynikało z jej nazwy :).

Jeśli myślisz, że to technologia zarezerwowana dla informatyków z topowych firm technologicznych, na następnych stronach tej książki wyprowadzę Ciebie z błędu. Każdy – nawet Ty – może stać się mistrzem szyfrowania. I nie, nie potrzebujesz do tego doktoratu z kryptografii, ani nawet jakiejkolwiek innej zaawansowanej dziedziny wiedzy.

Technologia daje nam odpowiednie narzędzia. Ale pojawiają się różne ograniczenia i to co najmniej dwa są istotne na początku Twojej drogi 😉:

- Twoja dobra wola do zainteresowania się tematem szyfrowania (i kryptografii),
- Czas, bo szybkość jest wrogiem bezpieczeństwa, czyli także szyfrowania, a Ty już wkrótce to zrozumiesz - o ile zagłębisz się w kolejne strony tego poradnika.

2. DLACZEGO WARTO ZGŁĘBIĆ TAJNIKI SZYFROWANIA?

Każdego dnia korzystamy ze wspaniałych technologii, które wymieniają się informacjami – od wysyłania maili po przechowywanie plików w tak zwanej "chmurze IT" lub po prostu "chmurze". Ale w świecie, gdzie dane są nową walutą, każdy błąd może kosztować więcej, niż się spodziewasz.

Szyfrowanie to wcale nie jest żaden luksus – to podstawowe narzędzie w cyfrowym świecie. W tej książce pokażę Ci, jak prosto i skutecznie wprowadzić szyfrowanie do Twojego życia zawodowego i osobistego.

Co znajdziesz w Części 1 serii: Szyfrowanie Bezpieczeństwo?

Przygotowałem dla Ciebie przewodnik, którego pierwsze dwie części - krok po kroku - przeprowadzą Ciebie przez podstawy szyfrowania. Całość poradnika podzieliłem na moduły, z których każdy skupia się na innym aspekcie.

Nie bój się – prawie wszystko wyjaśnione jest prosto, zrozumiale, a czasem nawet z odrobiną humoru. Bo kto powiedział, że o bezpieczeństwie, szyfrowaniu i kryptografii - nie można pisać z szerokim uśmiechem na twarzy?

CZĘŚĆ 1 to wprowadzenie do podstaw

1. **Podstawy szyfrowania**:

   Na początek dowiesz się, czym jest szyfrowanie, skąd się wzięło i dlaczego jest tak ważne. Przygotuj się na kilka ciekawostek z historii – od Cezara po współczesne algorytmy.

2. **Symetria i asymetria – szyfrowanie na dwa sposoby**:

   Poznasz dwa podstawowe rodzaje szyfrowania, ich zalety, wady i zastosowania w codziennej praktyce. Zrozumiesz, dlaczego tak zwane klucze: publiczne i prywatne - to jak yin i yang w świecie kryptografii.

CZĘŚCI: 2, 3 i następne (tak, przewidziałem ich sporo :)) - zajmą się kolejnymi niezmiernie ważnymi elementami szyfrowania, o których dowiesz się zapewne w części drugiej, do której już teraz Ciebie zapraszam.

Ale pozwól, że nakreślę obszary wiedzy, które zamierzam poruszyć w kilku kolejnych Modułach:

- **Protokoły szyfrowania**
- **Praktyczne zastosowania szyfrowania**
- **Typowe błędy i najlepsze praktyki**
- **Szyfrowanie w biurze**
- **Szyfrowanie aplikacji biurowych**

i wiele innych związanych z szyfrowaniem oraz cyfrowym bezpieczeństwem.

3. DLACZEGO TA SERIA KSIĄŻEK JEST INNA?

Moim celem było stworzenie poradnika, który nie tylko dostarcza wiedzy, ale też zachęca do działania. Znajdziesz tu nie tylko przydatne teorie, ale przede wszystkim praktyczne przykłady, wskazówki i – co najważniejsze – lekki styl, który pozwoli Ci przyswajać wiedzę z uśmiechem na twarzy. A ponieważ w ponad 90% (lub coś koło tego :)) skupiam się na rozwiązaniach open source oraz bezpłatnych, więc każdy i każda z Was będzie mógł/mogła w praktyce zobaczyć oraz przećwiczyć większość z omawianych elementów szyfrowania.

Chcę, żebyś po przeczytaniu tej książki pomyślał/a: „To było łatwiejsze, niż myślałem/am!” i od razu zaczął/ęła stosować szyfrowanie w praktyce. A ponieważ szyfrowania to jeden z filarów cyberbezpieczeństwa, więc po poznaniu i zrozumieniu zagadnień poruszanych w tej serii ebooków - Twoja wartość na rynku pracy zapewne znacząco się zwiększy.

Jak już wspomniałem nacisk będę kładł na szyfrowanie a nie na kryptografię. Jednakże jak już wkrótce się dowiesz - szyfrowanie to jedynie element kryptografii. Ale na początkowym etapie nauki, warto zgłębić właśnie sztukę szyfrowania, aby potem móc spojrzeć na całość problemu, czyli z punktu widzenia kryptografii. Nie oznacza to, że nie będzie już w pierwszej części elementów wiedzy kryptograficznej wychodzących poza samo tylko szyfrowanie. Tak się nie da, choćby ze względów technologicznych, gdzie zastosowanie szyfrowania opiera się także o aspekty całej kryptografii czyli mam na myśli: poufność, integralność, uwierzytelnienie, niezaprzeczalność. Na wyjaśnienie tych czterech pojęć zapraszam Ciebie do dalszej części mojego poradnika.

4. DLA KOGO JEST TA KSIĄŻKA?

W mojej opinii, ten poradnik jest dla każdej osoby, która ma do czynienia z urządzeniami typu: komputer, smartfon, tablet. A czy są jeszcze ludzie, którzy nie używają choćby jednego z wyżej wymienionych narzędzi cyfrowych?

Niezależnie od tego, czy jesteś pracownikiem/cą biurowym/ą, freelancerem/ką, studentem/ką czy właścicielem/ką firmy – jeśli zależy Ci na bezpieczeństwie danych, ta książka jest dla Ciebie. Nawet jeśli dopiero zaczynasz swoją przygodę z szyfrowaniem, znajdziesz tu wszystko, czego potrzebujesz, by ruszyć z miejsca.

Gotowy/a na podróż po świecie szyfrowania? Świetnie! Weź kubek kawy, zrelaksuj się i zacznijmy wspólnie ze mną odkrywać tajniki bezpieczeństwa danych oraz wielu innych obszarów cyberbezpieczeństwa. Obiecuję, że będzie: ciekawie, praktycznie i czasami … całkiem zabawnie. 😊

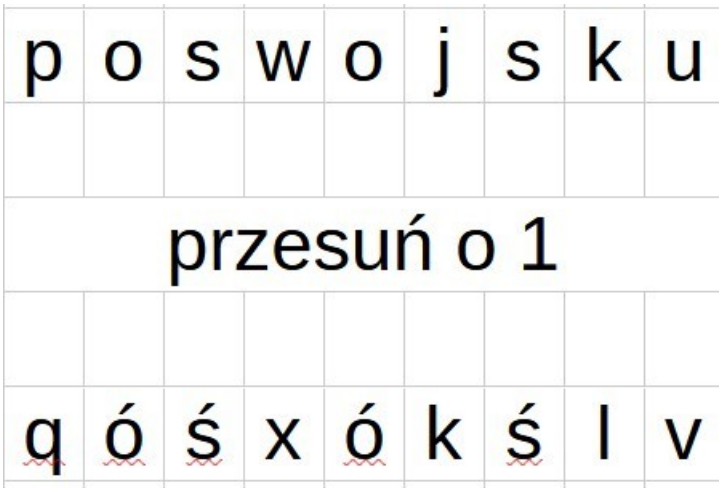
Moduł 1: PODSTAWOWE POJĘCIA I KONCEPCJE SZYFROWANIA

1. DEFINICJA I HISTORIA SZYFROWANIA

Co to jest szyfrowanie?

Wyobraź sobie, że masz sekretny dziennik i nie chcesz, żeby ktokolwiek inny go czytał. Piszesz go w tajnym języku, który tylko Ty rozumiesz. Czyli robisz ... szyfrowanie! Dokładnie tym zajmiemy się w tym poradniku, tylko że w wersji cyfrowej!

Szyfrowanie polega na przekształceniu posiadanych informacji w taki sposób, że bez specjalnego "klucza" nikt ich nie odczyta lub dokładniej rzecz biorąc w prosty sposób odczytać nie będzie w stanie. Jednakże pamiętajmy, że zabezpieczenia, które stworzył człowiek, także człowiek może pokonać :). Ale nie wchodźmy od razu w tzw. hakowanie. Przyjdzie na to pora. Zerknij poniżej - na zdjęcie. Jest na nim pokazana jedna z najstarszych metod szyfrowania - Szyfr Cezara. Wkrótce wyjaśnię go kompleksowo, teraz jedynie chciałbym abyś ujrzał/a tak zwany tekst źródłowy oraz tekst (a właściwie ciąg znaków), który powstał w wyniku zaszyfrowania tekstu źródłowego. W tym przypadku kluczem jest liczba 1, która przesuwa się w prawo po alfabecie. To jedna z najprostszych metod i jak już wspomniałem jedna z najstarszych znanych ludzkości.



Zdjęcie: przykład zaszyfrowania wyrazu poswojsku

Szyfrowanie to proces, czynność - przekształcania czytelnych danych (tekst jawny, np: "poswojsku") w **formę nieczytelną** (tekst zaszyfrowany "qóśxókślv"), aby zapewnić ich poufność. Dokonane to musi być według jakiejś określonej metodologii. Odzyskanie pierwotnej formy danych wymaga znajomości specjalnego klucza (metodologia) i zwykle choć odrobiny inteligencji :). W tym przypadku kluczem jest znajomość alfabetu i przesunięcia zawartości tekstu jawnego (kolejnych literek) w prawo. Szyfrowanie to jedna z podstawowych technik ochrony informacji przed nieautoryzowanym dostępem. Warto dodać, że dobrze wykonana, może być bardzo skuteczna.

Rozwińmy definicję

Wyobraź sobie, że wysyłasz jakiś list do znajomego, ale nie chcesz, żeby ktokolwiek inny go przeczytał. Szyfrowanie to jak zamknięcie listu w sejfie, do którego tylko odbiorca ma klucz.

Niby proste i oczywiste. Mam na myśli powyższy opis szyfrowania. W świece rzeczywistym, prawie wszyscy dbamy o zabezpieczanie naszego majątku i innych zasobów. Niestety, świat cyfrowy wiele osób traktuje zupełnie inaczej. Ja tego nie rozumiem, bo jak można być odpowiedzialnym w świecie rzeczywistym, a zupełnie ignorować odpowiedzialność w cyber świecie?

Krótka historia szyfrowania

Szyfrowanie towarzyszyło ludzkości od .. hmm, chyba tak zwanego: "zarania dziejów". Dawno, dawno temu - techniki szyfrowania były prawdopodobnie dużo mniej skomplikowane niż w czasach obecnych. Tak przynajmniej wynika z zapisków historycznych. Choć, aby to stwierdzić tak zupełnie jednoznacznie, musielibyśmy się przenieść do tamtych - pradawnych czasów. A to wydaje się być niemożliwe :).

Zauważ, że pomysłowość w ukrywaniu różnorodnych informacji wynikała i zapewne ciągle wynika - z potrzeby ochrony sekretów:

- wojskowych,
- handlowych,
- osobistych,
- finansowych,
- politycznych,
- i zapewne wielu, wielu innych.

W ubiegłych stuleciach a nawet tysiącleciach - zapewne było podobnie. Istnieje wiele historycznych sposobów szyfrowania, które do dnia dzisiejszego są znane i - głównie w celach naukowych - ciągle jeszcze używane. Jednym z nich jest wspomniany już Szyfr Cezara, który stał się jednym z najbardziej rozpoznawalnych. Zapewne stało się tak dzięki jego prostocie oraz skuteczności - prze wiele lat uznawany był za szyfr nie do złamania. Poniżej znajdziesz informacje na temat kilku historycznych rodzajach szyfrowania.

Skoro wspominałem już wcześniej o jednym z najsłynniejszych sposobów szyfrowania, to rozpocznijmy od niego i jeszcze dwóch równie znanych, a potem - w skrócie wspomnę o kilku innych w układzie chronologicznym - od najstarszego.

- W czasach starożytnych Rzymianie mieli swoją wersję "super tajnego języka" – **szyfr Cezara**. Polega on na przesuwaniu liter w alfabecie o kilka miejsc. Dla przykładu wyraz "poswojsku" po zastosowaniu omawianej metody i uwzględniając tzw. polskie fonty oraz tzw. litery w nieprzyswojonych wyrazach, zamienia się w "qóśxókślv", czyli:
    - p na q
    - o na ó
    - s na ś
    - w na x
    - o na ó
    - j na k
    - s na ś
    - k na l
    - u na v

- W średniowieczu stosowano bardziej skomplikowane szyfry, jak np. szyfry podstawieniowe, gdzie każda litera miała swój odpowiednik.
- W czasie II wojny światowej pojawiły się maszyny szyfrujące, takie jak **Enigma** – kluczowy element wśród technologii wywiadowczych.
- Dziś mamy **algorytmy matematyczne**, takie jak AES czy RSA, które zapewniają bezpieczeństwo w świecie cyfrowym. I tak, działają lepiej niż szyfr Cezara! 😉

W kolejnych modułach tej serii poradników omówię wiele ciekawych sposobów szyfrowania. A w oparciu o:

- posiadaną wiedzę oraz
- informacje znalezione w Wikipedii,

opracowałem poniżej kilka opisów ciekawych, historycznych metod szyfrowania.

Historia szyfrowania

Mezopotamia i gliniane tabliczki (ok. 1500 p.n.e., choć społeczeństwo Summerowów to jakieś 4000 p.n.e)

W Mezopotamii znaleziono tabliczki zawierające tajemnicze formuły chemiczne, a przynajmniej tak podejrzewają naukowcy w latach obecnych. Mogły one ponoć dotyczyć produkcji ceramiki i szkła. Informacje te były zapewne celowo zapisywane w sposób utrudniający ich zrozumienie przez osoby postronne. Ale jakbyśmy sięgnęli 3-4 tysiące lat p.n.e, to także w artefaktach pozostałych po wspaniałej sumeryjskiej cywilizacji, znaleźlibyśmy dowody na istnienie szyfrowania pra starożytnych informacji. A może nawet jeszcze dużo starszych ;).

Egipt i hieroglify (jakieś 1000-2000 p.n.e.)

W starożytnym Egipcie kapłani i tak zwani skrybowie (osoby zajmujące się zawodowo odręcznym przepisywaniem ksiąg lub dokumentów) tworzyli alternatywne formy hieroglifów, aby ukryć znaczenie tekstów religijnych lub administracyjnych. Były one zapewne bardziej złożone oraz trudniejsze do zrozumienia dla przeciętnego Egipcjanina.

Ponoć w grobowcach używano „pseudo-hieroglify”, które były rodzajem zakodowanych inskrypcji. Swoją drogą ciekawe, co chcieli nam - ich potomkom - przekazać? A może jakieś informacje o praprzodkach kosmitach? ;) Ale "zejdźmy na Ziemię" :) i może lepiej nie idźmy w kierunku rozważań filozoficzno-kosmicznych. Na to przyjdzie może pora w kolejnych częściach poradnika lub w zupełnie innej książce ;).

Sparta i skytale (ok. 500 p.n.e.)

Skytale to prawdopodobnie najstarsze znane narzędzie szyfrujące. Spartanie używali drewnianego walca oraz owiniętego wokół niego pasa pergaminu do zapisywania wiadomości. Tylko osoba posiadająca walec o takim samym rozmiarze mogła poprawnie odczytać wiadomość. Wizualizację Skytale możesz zobaczyć między innymi na stronach Wikipedii (https://pl.wikipedia.org/wiki/Skytale).

Hebrajski system Atbash (ok. 600 p.n.e.)

Atbash to stosunkowo prosty szyfr zamieniający litery alfabetu hebrajskiego w sposób „odwrócony” (A stawało się Z, B – Y itd.). Był stosowany między innymi w starożytnych tekstach religijnych, np. w Biblii. Więcej informacji na ten temat znajdziesz na stronach WIkipedii - źródło: https://pl.wikipedia.org/wiki/Atbasz.

Indie, Chiny i inne Państwa Azjatyckie (ok. kilkaset lat p. n.e.)

Azja oraz jej cywilizacje są chyba ciągle jednym z najmniej zbadanych obszarów z punktu widzenia wiedzy związanej z matematyką i obszarami jej pokrewnymi. Dotyczy to także szyfrowania. Ale jakbyś sięgnął/ęła do pism hinduistycznych (choćby tzw. Wed, np. Mahabharata) czy chińskiej myśli filozoficznej, tam także można znaleźć mnóstwo przykładów na wykorzystywanie ukrywania informacji pod przykrywką jawnych tekstów. Wystarczy się wczytać :).

Grecki szyfr Polibiusza (ok. 200- 118 p.n.e.)

Słynny Grecki historyk Polybius opisał system siatki 5 na 5 (tzw. kwadrat Polybiusza), który mógł być wykorzystywany do szyfrowania wiadomości za pomocą par cyfr. Więcej na ten temat znajdziesz między innymi na stronach Wikipedii (https://pl.wikipedia.org/wiki/Szachownica_Polibiusza).

Szyfr Cezara (I wiek p.n.e.)

Jak już wspominałem, jest to jeden z najbardziej znanych, historycznych szyfrów. Używany był przez Juliusza Cezara. Polegał na przesuwaniu liter w alfabecie o ustaloną liczbę miejsc. Opisałem to już wcześniej na konkretnym przykładzie "poswojsku".

Szyfr Vigenere'a (XVI wiek)

Ta metoda pochodzi ze Średniowiecza. Jej autorstwo przypisywane jest francuskiemu dyplomacie, choć sprawa jest nieco zagmatwana. Ale ponieważ jesteśmy w podstawach szyfrowania, a nie w rozprawce historycznej, pozwól, że nie odniosę się do szczegółów tej sprawy. Poza tym możesz w każdej chwili sięgnąć po szczegóły do źródeł, np. wcześniej wspominanej już kilka razy Wikipedii - adres:
https://pl.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re.

Omawiany sposób szyfrowania wprowadza element zmienności poprzez stosowanie hasła, które określało sposób szyfrowania każdej litery. Co jest tutaj bardzo ciekawe? Ten sposób szyfrowania przetrwał swoje czasy. Był uznawany za niełamliwy przez jakieś 300 lat. Nieźle, prawda?

Maszyna szyfrująca Enigma (XX wiek)

Legendą obrosły spory kto rozszyfrował Enigmę: Polacy, Brytyjczycy, a może .. Eech, jak wspomniałem nie jest to rozprawka historyczna :). Przechodząc do meritum - Enigma używana była przez Niemcy w czasie II wojny światowej. Była niezwykle skomplikowana, ale złamana przez matematyków z zespołu Alana Turinga (kimkolwiek by nie byli :)), co miało ogromny wpływ na wynik wojny.

Algorytm DES (Data Encryption Standard, 1977)

Algorytm DES został wprowadzony jako standard szyfrowania w USA. Był to jeden z pierwszych szeroko stosowanych algorytmów szyfrowania symetrycznego. Obecnie jest uważany już jako przestarzały.

RSA (Rivest-Shamir-Adleman, 1978)

Jeden z pierwszych praktycznych algorytmów szyfrowania asymetrycznego, a może nawet pierwszy? Wykorzystuje on pary kluczy: publiczny i prywatny. Jest podstawą współczesnej kryptografii. O tym będziemy się wspólnie całkiem sporo uczyć. Już za dłuższą chwilkę :). A o RSA trzeba wiedzieć, że także jest już uważany za przestarzały i chyba nawet nieco niebezpieczny.

AES (Advanced Encryption Standard, 2001)

AES bezpośrednio zastąpił DES jako nowoczesny standard szyfrowania symetrycznego. Tak przynajmniej jest na dzień pisania tego zdania :). AES jest szybki i bezpieczny, dlatego jest bardzo szeroko stosowany, między innymi w: bankowości, Wi-Fi, aplikacjach webowych i mobilnych.

Szyfrowanie end-to-end (E2EE, XXI wiek)

Na dzisiaj to zupełny hicior! Szyfrowanie end-to-end wprowadzone zostało w komunikatorach takich jak Signal czy WhatsApp. Zapewnia, że tylko nadawca i odbiorca mogą odczytać wiadomości, nawet dostawca usługi nie ma do nich dostępu. Przynajmniej taką my - użytkownicy mamy nadzieję. Warto wiedzieć, że nie wszystkie popularne komunikatory używają tego rozwiązania, ale szczegóły znajdziesz dalej, w kolejnych modułach.

Zdjęcie - źródło: signal.org

Post-quantum cryptography (współczesność)

Wchodzimy w świat kwantowy. Kryptografia kwantowa kiedyś zmieni świat. A właściwie praktyczne wykorzystanie komputerów kwantowych zmieni świat. Na dzisiaj pewnym jest, że obecnie używane metody kryptografii nie sprostają pod względem bezpieczeństwa komputerom kwantowym. Właśnie dlatego opracowywane są nowe algorytmy, takie które będą odporne na ataki komputerów kwantowych. Kiedyś, w przyszłości - kryptografia kwantowa stanie się standardem. Kiedyś, czyli ..., hmm, za kilka lat? A może szybciej?

Szyfrowanie dokonywane przez AI - Sztuczną Inteligencję

Obecne systemy szyfrowania stworzył człowiek, ale teraz pora na AI i jej efekty pracy w tym zakresie. A co uzyskamy? Czas pokaże. Obyśmy tylko byli w stanie to zrozumieć i zobaczyć, bo może AI uzna, że nie jesteśmy - my ludzie - już potrzebni na Ziemi? ;(

2. DLACZEGO SZYFROWANIE JEST KLUCZOWE W CYBERBEZPIECZEŃSTWIE?

Twoje dane to prawdziwy, unikalny skarb!

Zastanów się: czy chciałbyś/abyś, żeby ktokolwiek bez pozwolenia:

- Czytał Twoje dokumenty, e-maile?
- Przeglądał Twoje prywatne zdjęcia czy filmy?
- Przejął dostęp do Twojego konta bankowego?

Szyfrowanie jest jak zamek w drzwiach do domu – chroni Twoje dane przed nieproszonymi gośćmi.

Wyobraź sobie, że twoje zasoby – hasła, zdjęcia, e-maile – to bezcenne skarby. Nie mówimy tu o złotych monetach (chociaż kto wie, co masz na dysku! :), może bitcoiny?), ale o czymś równie cennym: Twojej prywatności i bezpieczeństwie w sieci.

Szyfrowanie to strażnik tych skarbów – taki wojownik, który chroni zamek pełen kosztowności przed nieproszonymi gośćmi.

Co to jest szyfrowanie i jak się ma do kryptografii?

Szyfrowanie to proces zamieniania Twoich informacji w coś, co przypomina .. może język kosmitów? W każdym razie szyfrowanie powinno doprowadzić do powstania "nieczytelnego bełkotu", z którego nic sensownego nie wynika. Dopiero posiadanie odpowiedniego "klucza" (czyli specjalnego hasła lub kodu) pozwala odczytać ze zrozumieniem tę wiadomość.

Wyobraź sobie, że wysyłasz list do znajomego, ale zamiast słów, używasz jakiegoś tajemniczego szyfru. Tylko Ty i Twój znajomy wiecie, jak go odszyfrować. Dla każdego innego list wygląda jak dziwaczne bazgroły! Całkiem jakbyś rozum postradał/a w trakcie pisania tego dokumentu :).

Szyfrowanie i kryptografia są ze sobą bardzo powiązane, ale różnią się zakresem, którym się zajmują.

SERDECZNIE ZAPRASZAM DO NABYCIE PEŁNEJ WERSJI TEGO PORADNIKA :)

pozdrawiam:

Autor Dariusz Gołębiowski

PODSUMOWANIE: OD AUTORA

Drodzy Czytelnicy,

Dotarliście do końca tej pierwszej części serii

„SZYFROWANIE BEZPIECZEŃSTWO: CZĘŚĆ 1 Podstawowe pojęcia i koncepcje”,

która została stworzona, by wprowadzić Was w świat ochrony danych w sposób prosty, przystępny i praktyczny. Mam nadzieję, że po lekturze czujecie się pewniej w omawianym temacie szyfrowania i widzicie, że to nie jest wyłącznie domena informatyków w laboratoriach czy specjalistów z tajnych służb.

Czego nauczyliśmy się w tej części?

W siedmiu modułach przeszliśmy przez kluczowe fundamenty szyfrowania, które stanowią bazę dla bardziej zaawansowanych zagadnień w przyszłości. Oto, co udało nam się wspólnie osiągnąć:

1. **Zrozumieliśmy, czym jest szyfrowanie i dlaczego jest tak ważne.**

   Poznaliśmy historię i zastosowania szyfrowania – od starożytnych kodów Cezara po współczesne algorytmy, które chronią nasze dane każdego dnia.

2. **Poznaliśmy różne rodzaje szyfrowania.**

   Symetryczne i asymetryczne – dowiedzieliśmy się, kiedy stosować które z nich i jakie narzędzia są z nimi związane.

Zrozumieliśmy, jakie pułapki mogą czyhać na początkujących i jak ich unikać, by szyfrowanie było skuteczne.

Co dalej?

Ten eBook jest jedynie wstępem, pierwszym krokiem na drodze do pełniejszego zrozumienia szyfrowania i bezpieczeństwa danych. To fundamenty, na których możecie budować swoją wiedzę. Kolejne części serii zabiorą Was w głąb bardziej zaawansowanych zagadnień, takich jak:

- Szczegółowe zastosowanie algorytmów szyfrowania w różnych środowiskach.
- Zaawansowane narzędzia i techniki ochrony danych.
- Szyfrowanie baz danych, aplikacji i systemów w bardziej wymagających scenariuszach.

Ode mnie dla Was

Mam nadzieję, że ta książka nie tylko dostarczyła Wam wiedzy, ale również zainspirowała do działania. Szyfrowanie to coś więcej niż technologia – to sposób na przejęcie kontroli nad swoimi danymi i ochrona tego, co dla nas ważne. Jestem przekonany, że każdy z Was, niezależnie od wcześniejszego doświadczenia, może wdrożyć tę wiedzę w swoim życiu.

Dziękuję, że zdecydowaliście się na ten pierwszy krok. Trzymam za Was kciuki i zapraszam do kolejnych części serii, gdzie zanurzymy się jeszcze głębiej w świat bezpieczeństwa danych. 😊

Powodzenia w chronieniu Waszych danych – w końcu nikt nie zrobi tego lepiej niż Wy sami!

Wasz przewodnik po świecie szyfrowania,

Autor: Dariusz Gołębiowski

Informacje o prawach autorskich

W poradniku wykorzystano:

- własne materiały graficzne,
- prace graficzne AI: Chat GPT4,
- cliparty z programu LibreOffice na licencji CCO.

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika: DARIUSZ GOŁĘBIOWSKI

Zapraszam do zapoznania się z innymi książkami, które napisałem lub współtworzyłem.


TWOJE BEZPIECZEŃSTWO
W ŚWIECIE CYBER
I SZTUCZNEJ INTELIGENCJI
Część I
Wprowadzenie
TWOJE BEZPIECZEŃSTWO
W ŚWIECIE CYBER
I SZTUCZNEJ INTELIGENCJI
Część II
Cyberhigiena
TWOJE BEZPIECZEŃSTWO
W ŚWIECIE CYBER
I SZTUCZNEJ INTELIGENCJI
Część III
Dziecko i Ty
AI W EDUKACJI
Część 1
AI
praktyczny poradnik
nie tylko dla nauczycieli
AI W EDUKACJI
Część 2
AI
praktyczne pomysły
na kreatywną naukę
Wydawnictwo Cyfrowe poswojsku.pl
www. poswojsku.pl

Więcej informacji znajdziesz na stronach firmy:

Wydawnictwo Cyfrowe poswojsku.pl

www.poswojsku.pl

* ***„CHROŃ I ROZWIJAJ BIZNES – CYBER AI Część 1 Wykorzystanie AI w bezpieczeństwie organizacji”*** .
* ***„AI W EDUKACJI Część 1 Praktyczny poradnik nie tylko dla nauczycieli”*** .
* ***„AI W EDUKACJI Część 2 Praktyczne pomysły na kreatywną naukę”*** .
* ***„TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER ORAZ SZTUCZNEJ INTELIGENCJI Część 1 Wprowadzenie”***.
* ***„TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER ORAZ SZTUCZNEJ INTELIGENCJI Część 2 Cyberhigiena”***.
* ***„TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER ORAZ SZTUCZNEJ INTELIGENCJI Część 3 Dziecko i Ty***”.
* ***„Stwórz Grę Mobilną Wydanie 2”, aktualizacja 2023 (ebook) - poradnik kodowania gry mobilnej w języku programowania: JavaScript – framework React Native.***

Prawa autorskie i znaki towarowe: