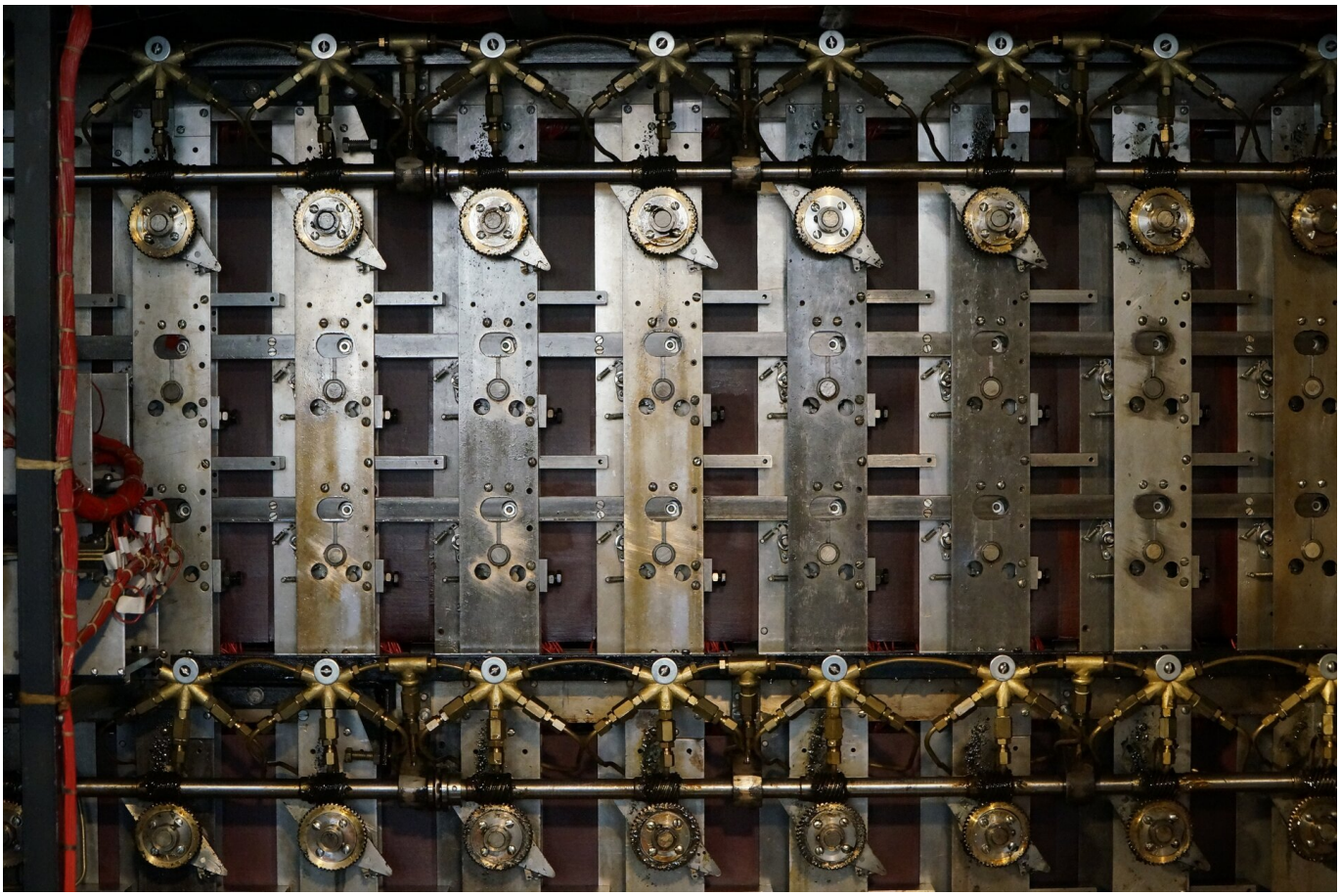


Szyfry symetryczne i asymetryczne

Źródło: awsloley, domena publiczna.

Szyfry zabezpieczające, o których możesz więcej przeczytać w e-materiale Wstęp do kryptografii, mają za zadanie chronić poufne informacje. Działają one analogicznie do zamków w drzwiach, zabezpieczających domy przed nieproszonymi gośćmi. Do otwarcia lub zamknięcia zamka potrzebujemy klucza, podobnie jest w wypadku szyfrów – potrzebujemy klucza by zaszyfrować lub odszyfrować wiadomość. W zależności od tego, jaki typ szyfru zastosujemy, szyfrowanie i deszyfrowanie odbywać się może za pomocą jednego lub dwóch kluczy. W tym e-materiale poznamy dwa typy szyfrów: symetryczne oraz asymetryczne.

Implementacje omawianych szyfrów przedstawiamy w e-materiałach:

- Szyfry symetryczne i asymetryczne w języku C++,
- Szyfry symetryczne i asymetryczne w języku Java,
- Szyfry symetryczne i asymetryczne w języku Python.

Więcej zadań? Sięgnij do: Szyfry symetryczne i asymetryczne – zadania maturalne.

> **Twoje cele**
>
> - Wymienisz różnice pomiędzy szyframi symetrycznymi i asymetrycznymi.
> - Rozpoznasz główne wady i zalety poszczególnych rodzajów szyfrowania.
> - Scharakteryzujesz klucze publiczny oraz prywatny.

- Przeanalizujesz proces szyfrowania danych podczas przesyłania.

Przeczytaj

Szyfry symetryczne

Pierwszym rodzajem szyfrów, który omówimy, będą szyfry symetryczne. Charakteryzują się one stosowaniem jednego klucza, zarówno do procesu szyfrowania, jak i deszyfrowania. Takie rozwiązanie jest szybkie i wygodne, ale nie możemy zapominać o kwestiach bezpieczeństwa. W obu przypadkach, gdy klucz dostanie się w niepowołane ręce, może to doprowadzić do potencjalnie niebezpiecznych sytuacji.

Przekazując klucz, musimy zachować odpowiednie środki zabezpieczeń. W wypadku szyfru symetrycznego dodatkowe zagrożenie wynika z dzielenia sekretu przez nadawcę i odbiorcę wiadomości. Prawdopodobieństwo dostania się klucza w niepowołane ręce jest wówczas znacznie większe, niż gdyby znała go tylko jedna osoba. Przechwycenie takiej informacji jest niebezpieczne również dlatego, że umożliwia postronnej osobie nie tylko rozszyfrowanie tajnych danych, lecz także samodzielne szyfrowanie wiadomości, a następnie wysyłanie ich do odbiorcy. Jeżeli ten odbiorca nie jest świadomy tzw. wycieku, przyjmie fałszywą wiadomość jako prawdziwą.

Rodzaje szyfrów symetrycznych

Szyfry symetryczne dzielimy na dwie grupy:

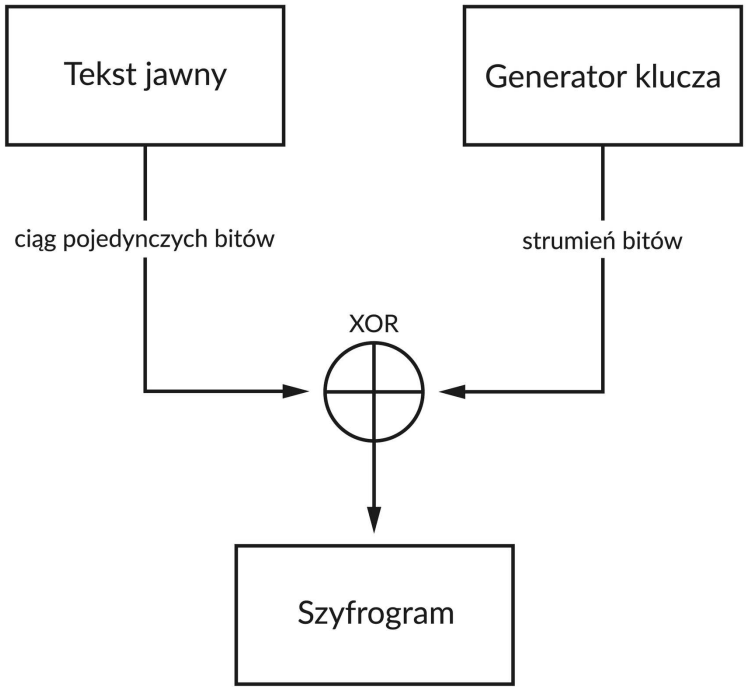
- Szyfry strumieniowe – ich głównym założeniem jest wygenerowanie strumienia bitów będącego kluczem, a następnie – z jego użyciem – szyfrowania po kolei każdego bitu tekstu jawnego. W praktyce odbywa się to zwykle z użyciem operacji logicznej XOR pomiędzy konkretnymi bitami wiadomości oraz odpowiadającymi im bitami klucza.
- Szyfry blokowe – opierają się na podzieleniu tekstu jawnego na bloki o identycznej długości np. 8 bajtów, a następnie – po kolei – szyfrowaniu ich z użyciem klucza. W wyniku tej operacji otrzymamy zaszyfrowane bloki tej samej długości.

Analiza algorytmów symetrycznych

Przykładów algorytmów symetrycznych jest wiele, aby zrozumieć główne założenia rządzące tą grupą, przeanalizujmy wspomniane dwa rodzaje szyfrów. Rozpoczniemy od algorytmu szyfrowania strumieniowego.

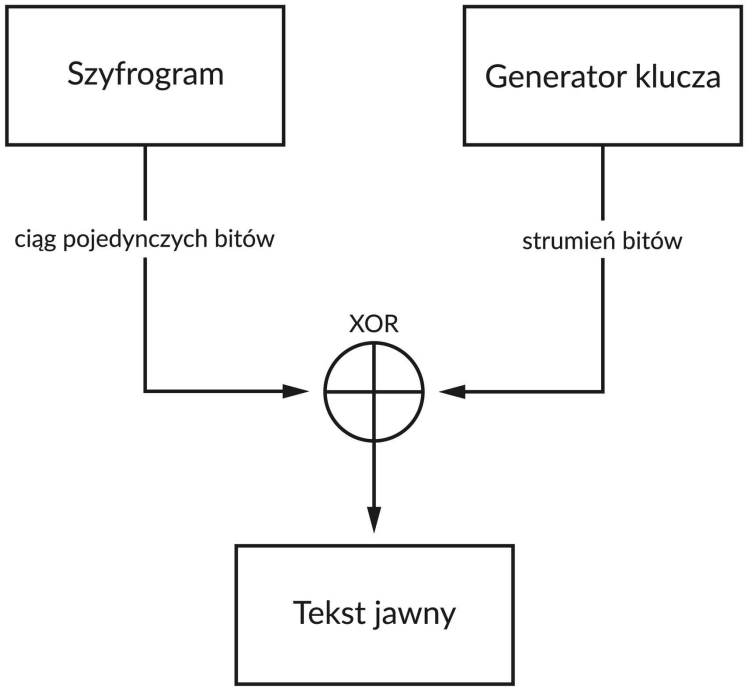
> **Przykład 1**
>
> Tak jak już wspominaliśmy, aby uzyskać szyfrogram, w wypadku algorytmów strumieniowych niezbędne jest zwykle przeprowadzenie operacji logicznej XOR pomiędzy tekstem jawnym oraz kluczem. W tym celu najpierw rozkładamy wartości

wejściowe do postaci ciągu pojedynczych bitów. W wypadku klucza stosujemy generator strumienia, natomiast tekst jawny, niezależnie od jego formy, prezentujemy w postaci binarnej. Operacja XOR przeprowadzana jest pomiędzy kolejnymi bitami tekstu jawnego oraz strumienia klucza. Powstały w ten sposób nowy ciąg bitów jest naszym szyfrogramem.



Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

Proces deszyfrowania jest analogiczny – danymi wejściowymi są szyfrogram oraz ten sam wygenerowany strumień bitów. Tym razem w wyniku przeprowadzonej operacji XOR otrzymujemy tekst jawny.

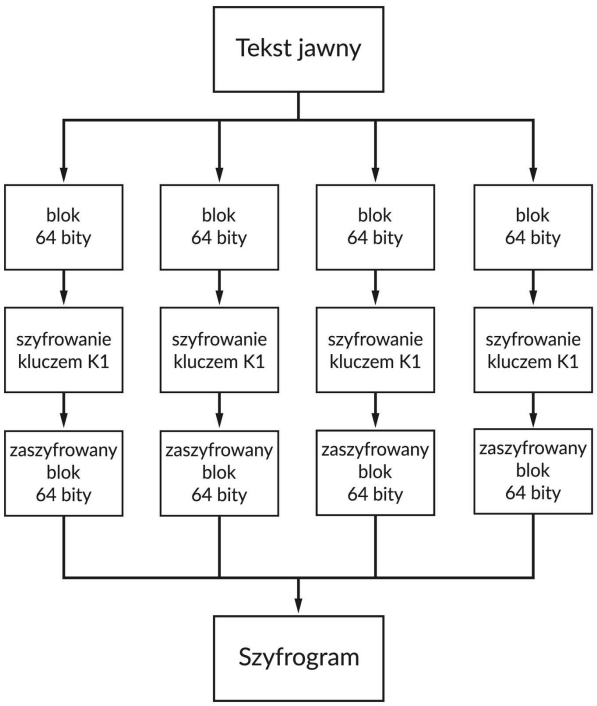


Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

W wypadku grupy szyfrów blokowych za przykład posłuży nam najprostszy tryb tego rodzaju szyfrowania – ECB (*Electronic codebook*). Bazuje on na dzieleniu tekstu jawnego na 64 bitowe bloki, a następnie oddzielne szyfrowanie każdego z nich tym samym kluczem.

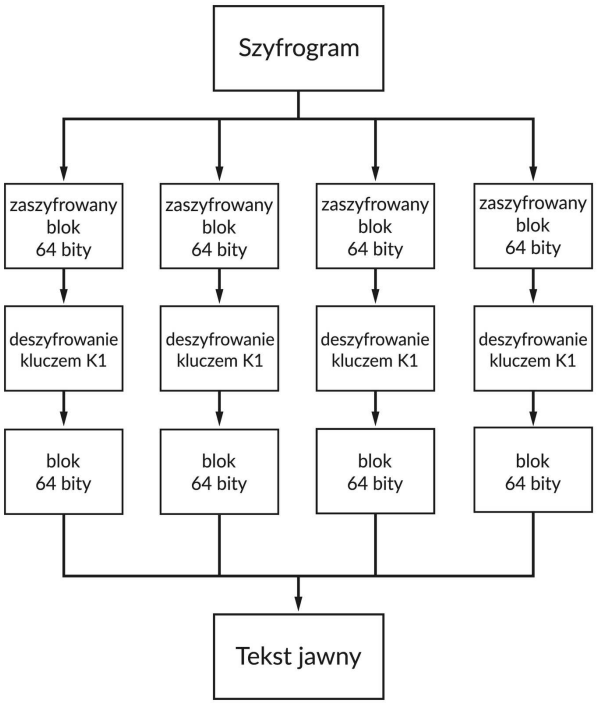
Przykład 2

Tekst jawny dzielimy na cztery bloki, każdy o wielkości 64 bitów. Za pomocą klucza K1 szyfrujemy osobno każdy z utworzonych bloków. W ten sposób otrzymaliśmy cztery zaszyfrowane bloki o wielkości 64 bitów. Po ich złożeniu otrzymujemy gotowy szyfrogram.



Źródło: Contentplus.pl sp. z o.o., licencja: CC BY-SA 3.0.

Deszyfrowanie odbywa się w sposób analogiczny. Szyfrogram ponownie rozdzielamy na bloki o wielkości 64 bitów, a następnie każdy z nich osobno deszyfrujemy z użyciem naszego klucza K1. W ten sposób otrzymujemy odszyfrowane bloki o tej samej wielkości. Po ich złożeniu mamy pełen tekst jawny.



Przykład

Przykładem szyfru symetrycznego jest szyfr XOR, ROT13, Cezara. Więcej na jego temat znajdziesz w e-materiałach:

- Szyfr Cezara,
- Szyfr Cezara w języku C++,
- Szyfr Cezara w języku Java,
- Szyfr Cezara w języku Python.

Szyfry asymetryczne

W wypadku szyfrów asymetrycznych operujemy dwoma osobnymi kluczami – jeden z nich jest szyfrujący, drugi – deszyfrujący. Są one zwykle określane jako klucze publiczny oraz prywatny. Przechwycenie klucza publicznego (szyfrującego) nie stanowi ryzyka, ponieważ nie daje on możliwości odszyfrowania zabezpieczonych wiadomości, a – co ciekawe – można go nawet udostępnić publicznie, by każdy zainteresowany miał możliwość zaszyfrowania wybranych przez siebie informacji.

Klucz prywatny (deszyfrujący) jest przetrzymywany w sekrecie i ma go tylko odbiorca wiadomości. W ten sposób znacznie redukujemy ryzyko, że dostanie się on w niepowołane ręce. Musimy jednak pamiętać, że w porównaniu do szyfrów symetrycznych, szyfry asymetryczne są bardziej skomplikowane, co powoduje, że operacje szyfrowania i deszyfrowania odbywają się znacznie wolniej. W systemach, w których zależy nam na czasie, powinniśmy zastosować szyfry symetryczne. Natomiast w wypadku, gdy naszym priorytetem jest bezpieczeństwo, wskazane jest pozostanie przy szyfrach asymetrycznych.

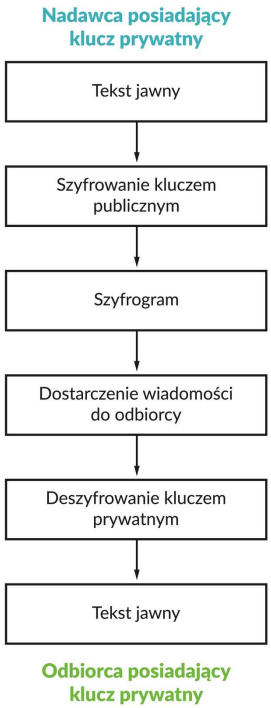
Oczywiście, większy poziom zabezpieczeń nie wyniknie tylko z głównych założeń tego typu szyfrów. Niezbędna jest odpowiednia konstrukcja kluczy, tak by osoba posiadająca klucz publiczny nie miała możliwości rozpracowania klucza deszyfrującego, opierając się jedynie na analizie tekstu jawnego i na odpowiadającym mu szyfrogramie.

Analiza algorytmów asymetrycznych

Przeanalizujmy schemat przedstawiający proces szyfrowania i deszyfrowania za pomocą szyfru asymetrycznego.

Przykład 3

Załóżmy, że nadawca posiada klucz publiczny pewnego szyfru asymetrycznego. Po przygotowaniu treści tekstu jawnego używa on uzyskanego klucza publicznego do zaszyfrowania wiadomości. W efekcie tej operacji otrzymał on szyfrogram. Po dostarczeniu zaszyfrowanej informacji, odbiorca używa swojego klucza prywatnego w procesie deszyfrowania. W ten sposób uzyskał on tekst jawny przygotowany przez nadawcę.



Szyfrowanie danych podczas przesyłania

Istotną kwestią w realiach transportu danych w internecie jest proces szyfrowania podczas przesyłania. Ma on na celu zabezpieczenie przesyłanych informacji przed ewentualnym podsłuchem przez m.in. innych użytkowników w tej sieci. W ten sposób nie będą oni w stanie dostać się do np. treści naszej wiadomości e-mail, a jedynie do stworzonego na jej podstawie szyfrogramu. Obecnie proces szyfrowania danych podczas przesyłania zapewnia

głównie protokół TLS (*Transport Layer Security*). Opiera się on na opisywanych podczas tej lekcji szyfrach asymetrycznych.

Przykład

Przykładem szyfru asymetrycznego jest szyfr RSA. Więcej na jego temat znajdziesz w e-materiałach:

- Szyfr RSA,
- Szyfr RSA w języku C++,
- Szyfr RSA w języku Java,
- Szyfr RSA w języku Python.

Słownik

> **klucz prywatny**
>
> rodzaj klucza, służącego w szyfrach asymetrycznych do deszyfrowania szyfrogramów; dostęp do niego powinien mieć tylko odbiorca zaszyfrowanych wiadomości
> **klucz publiczny**
>
> rodzaj klucza służącego w szyfrach asymetrycznych do szyfrowania tekstu jawnego; nie musi być utrzymywany w sekrecie, a nawet może zostać udostępniony publicznie
> **protokół TLS**
>
> protokół odpowiedzialny za zabezpieczania informacji transportowanych w sieci, oparty na szyfrach asymetrycznych

Gra edukacyjna

Polecenie 1

Sprawdź swoją wiedzę na temat szyfrów symetrycznych i asymetrycznych, biorąc udział w grze edukacyjnej.

Test

Sprawdź swoją wiedzę o szyfrach symetrycznych i asymetrycznych, biorąc udział w grze

Poziom trudności:

łatwy

Limit czasu:

7 min

Twój ostatni wynik:

-

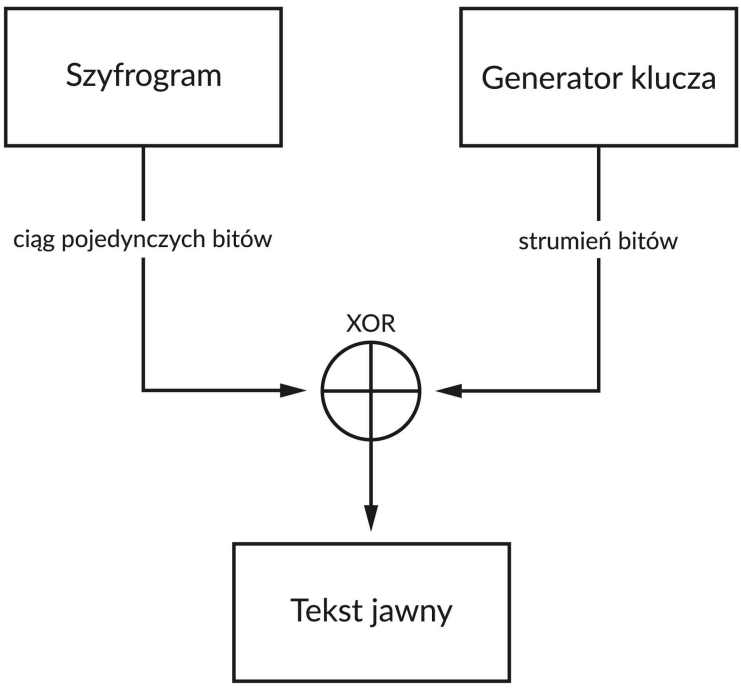
Uruchom

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Wskaż, co przedstawia poniższy schemat.



- Szyfrowanie w szyfrach symetrycznych
- Deszyfrowanie w szyfrach asymetrycznych
- Deszyfrowanie w szyfrach symetrycznych
- Szyfrowanie w szyfrach asymetrycznych

Ćwiczenie 2

Wybierz wszystkie poprawne odpowiedzi. Wraz z przyjacielem komunikujecie się, zabezpieczając swoje informacje szyfrem symetrycznym. Zaznacz, które z zagrożeń są realne, gdy postronna osoba przejmie używany przez was klucz.

- [ ] Otrzymana przez nas zaszyfrowana wiadomość może pochodzić od postronnej osoby, a nie przyjaciela.
- [ ] Żadne z wymienionych.
- [ ] Po przejęciu wiadomości z szyfrogramem osoba ta będzie w stanie go odszyfrować.

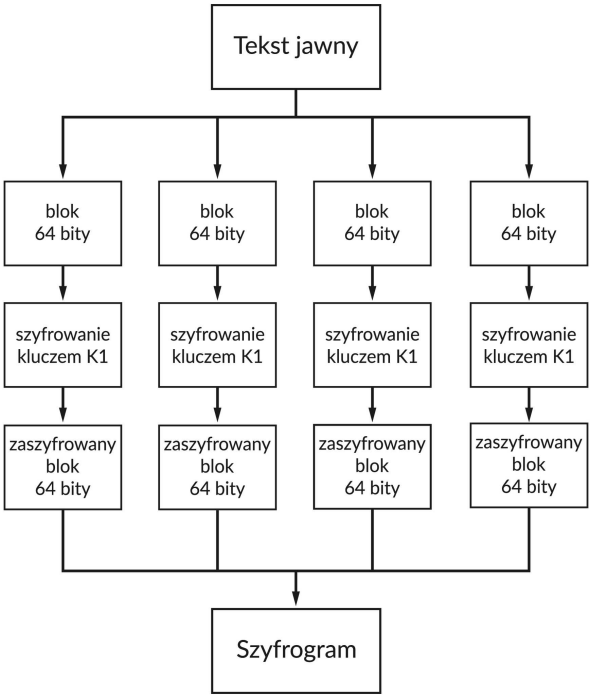
Ćwiczenie 3

Zaznacz wszystkie poprawne odpowiedzi. Wskaż, które z wymienionych pojęć są powiązane z kluczem publicznym.

- [ ] szyfrowanie
- [ ] szyfry symetryczne
- [ ] szyfry asymetryczne
- [ ] deszyfrowanie
- [ ] nadawca

Ćwiczenie 4

Zaznacz, czego nie przedstawia schemat



- [ ] deszyfrowania w trybie ECB
- [ ] szyfrowania w przykładowym szyfrze blokowym
- [ ] szyfrowania w przykładowym szyfrze strumieniowym
- [ ] szyfrowania w trybie ECB

Ćwiczenie 5

Uzupełnij tekst.

Istotną kwestią w realiach transportu danych w internecie jest proces _____ podczas przesyłania. Obecnie opisywany proces zapewnia głównie protokół o skrócie _____. Opiera się on na opisywanych podczas tej lekcji szyfrach _____.

Ćwiczenie 6

Uzupełnij tekst brakującymi informacjami.

Tryb _____ jest najprostszym trybem szyfrowania _____. Tekst jawny dzielony jest na _____ o długości 64 bitów. Każdy z nich jest osobno szyfrowany _____.

oddzielnym kluczem | tym samym kluczem | strumienie | ECB | bloki | blokowego | strumieniowego | OFB

Ćwiczenie 7

Zdania prawdziwe oznacz kolorem zielonym, a fałszywe kolorem czerwonym.

Zielony – zdania prawdziwe | Czerwony – zdania fałszywe

- Klucz prywatny nie powinien być udostępniany publicznie.
- W szyfrach asymetrycznych występują klucze prywatne, publiczne i uniwersalne.
- Najczęściej wykorzystywaną operacją logiczną w szyfrach strumieniowych jest AND.
- Szyfry symetryczne charakteryzują się dużą szybkością.

Ćwiczenie 8

Oznacz odpowiednim kolorem wymienione pojęcia. Weź pod uwagę, z którym rodzajem szyfrowania są powiązane:

Szyfry symetryczne | Szyfry asymetryczne | Szyfry symetryczne i asymetryczne

- Szyfry blokowe
- Szyfrogram
- Klucz publiczny
- Tekst jawny
- Generator strumienia bitowego

Dla nauczyciela

Autor: Maurycy Gast
Przedmiot: Informatyka

Temat: Szyfry symetryczne i asymetryczne

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

I. Rozumienie, analizowanie i rozwiązywanie problemów na bazie logicznego i abstrakcyjnego myślenia, myślenia algorytmicznego i sposobów reprezentowania informacji.

II. Programowanie i rozwiązywanie problemów z wykorzystaniem komputera oraz innych urządzeń cyfrowych: układanie i programowanie algorytmów, organizowanie, wyszukiwanie i udostępnianie informacji, posługiwanie się aplikacjami komputerowymi.

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

I. Rozumienie, analizowanie i rozwiązywanie problemów.

Zakres podstawowy. Uczeń:

2) stosuje przy rozwiązywaniu problemów z różnych dziedzin algorytmy poznane w szkole podstawowej oraz algorytmy:

b) na tekstach: porównywania tekstów, wyszukiwania wzorca w tekście metodą naiwną, szyfrowania tekstu metodą Cezara i przestawieniową,

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

3) objaśnia dobrany algorytm, uzasadnia poprawność rozwiązania na wybranych przykładach danych i ocenia jego efektywność;

I + II. Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

3) objaśnia, a także porównuje podstawowe metody i techniki algorytmiczne oraz struktury danych, wykorzystując przy tym przykłady problemów i algorytmów, w szczególności:

f) metodę szyfrowania z kluczem publicznym i jej zastosowanie w podpisie elektronicznym,

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

1) objaśnia rolę technik uwierzytelniania, kryptografii i podpisu elektronicznego w ochronie i dostępie do informacji;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Wymienisz różnice pomiędzy szyframi symetrycznymi i asymetrycznymi.
- Rozpoznasz główne wady i zalety poszczególnych rodzajów szyfrowania.
- Scharakteryzujesz klucze publiczny oraz prywatny.
- Przeanalizujesz proces szyfrowania danych podczas przesyłania.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- ćwiczenia praktyczne.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Szyfry symetryczne i asymetryczne". Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Prowadzący wyświetla na tablicy interaktywnej zawartość sekcji „Wprowadzenie" i omawia cele do osiągnięcia w trakcie lekcji.
2. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Nauczyciel ocenia, na podstawie informacji na platformie, stan przygotowania uczniów do zajęć. Jeżeli jest ono niewystarczające, prosi wybraną osobę o przedstawienie najważniejszych informacji z sekcji „Przeczytaj". Następnie na forum klasy uczniowie analizują przedstawione w niej rozwiązania Przykładów 1, 2 i 3.
2. **Praca z multimedium.** Uczniowie indywidualnie rozwiązują test sprawdzający ich wiedzę na temat szyfrów symetrycznych i asymetrycznych z sekcji „Gra edukacyjna".
3. Uczniowie w parach wykonują ćwiczenia nr 1-6 z sekcji „Sprawdź się". Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel zadaje pytania podsumowujące, np.
   – wskaż różnice pomiędzy szyframi symetrycznymi i asymetrycznymi?
   – jakie są główne wady i zalety danych rodzajów szyfrowania?
   – czym jest klucz publiczny oraz prywatny?
   – za co odpowiada protokół TLS?
2. Nauczyciel ponownie wyświetla na tablicy temat i cele lekcji zawarte w sekcji „Wprowadzenie". W kontekście ich realizacji następuje omówienie ewentualnych problemów z rozwiązaniem ćwiczeń z sekcji „Sprawdź się".

Praca domowa:

1. Uczniowie opracowują FAQ (minimum 3 pytania i odpowiedzi) do tematu lekcji („Szyfry symetryczne i asymetryczne").
2. Uczniowie wykonują ćwiczenia 7-8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Uczniowie mogą wykorzystać multimedium w sekcji „Gra edukacyjna" do przygotowania się do lekcji powtórkowej.