Szyfr RSA

- Wprowadzenie
- Przeczytaj
- Prezentacja multimedialna
- Sprawdź się
- Dla nauczyciela

Szyfr RSA

Źródło: Skitterphoto, dostępny w internecie: pixabay.com, domena publiczna.

Wysyłając prywatną wiadomość, chcemy mieć pewność, że nikt nieupoważniony jej nie przeczyta. Jak to osiągnąć, skoro we współczesnym świecie komputery stają się niewyobrażalnie szybkie i są w stanie przeprowadzać wybitnie złożone symulacje i analizy? Należy sięgnąć do rozwiązań z dziedziny matematyki, z których też korzysta algorytm RSA.

Algorytm RSA należy do szyfrów asymetrycznych – więcej informacji o nich znajdziesz w e-materiale: Szyfry symetryczne i asymetryczne.

Implementację omawianego algorytmu przedstawiamy w e-materiałach:

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

Więcej zadań? Sięgnij do: Szyfr RSA – zadania maturalne.

Twoje cele

- Wymienisz podstawowe różnice pomiędzy kluczem prywatnym a publicznym.
- Przeanalizujesz mechanizm wyznaczania klucza prywatnego i publicznego w algorytmie RSA.
- Wyjaśnisz, co to jest arytmetyka modularna i jak działa szyfr RSA.

Przeczytaj

Czym jest szyfr RSA?

> **Już wiesz**
>
> W wypadku szyfrowania asymetrycznego korzysta się z dwóch kluczy: publicznego do szyfrowania wiadomości oraz prywatnego – do odszyfrowania.

Nazwa szyfru RSA to skrót od nazwisk trzech profesorów z Massachusetts Institute of Technology w USA, którzy w 1977 r. opublikowali ten algorytm. Byli to Ronald L. Rivest, Adi Shamir i Leonard Adleman.

Szyfr RSA to asymetryczny algorytm kryptograficzny. Posiada parę kluczy – publiczny (e, n) oraz prywatny (d, n).
Postępowanie z użyciem asymetrycznego szyfrowania można sprowadzić do następujących kroków:

- Każda osoba, która chce otrzymać zaszyfrowaną wiadomość, „wystawia" na publiczny widok swój klucz publiczny.
- Osoba chcąca wysłać wiadomość szyfruje ją wykorzystując klucz publiczny osoby, do której chce ją wysłać.
- Osoba, która odbiera wiadomość, odszyfrowuje ją z użyciem swojego klucza prywatnego. Nikt, kto nie posiada klucza prywatnego, nie jest w stanie odszyfrować wiadomości.

Jak wyznaczyć klucz prywatny i publiczny?

1. Wybieramy dwie dowolne liczby pierwsze i oznaczamy je jako p i q. Liczby te powinny być możliwie jak największe.
2. Obliczamy wartość $n = p \cdot q$. Wartość n jest elementem klucza publicznego i prywatnego, określa również największą możliwą wielkość liczbową wysyłanej przez nas wiadomości.
3. Wyliczamy wartość funkcji Eulera dla n i wybieramy dowolną liczbę e spełniającą warunek $(1 < e < \varphi(n))$, która będzie względnie pierwsza do wartości $\varphi(n)$. Liczba e jest elementem klucza publicznego.
4. Obliczamy odwrotność modulo $\varphi(n)$ liczby e i otrzymujemy liczbę d, która jest elementem klucza prywatnego.

Po zrealizowaniu wszystkich czterech kroków możemy szyfrować i deszyfrować wiadomości zgodnie z następującymi funkcjami:

$$f(W) = W^e mod\, n$$

oraz:

$$f^{-1}(S) = S^d\ mod\, n$$

– gdzie W to wiadomość w postaci liczbowej, będąca mniejsza od n, a S to szyfrogram wiadomości, którą chcemy odszyfrować.

> **Ważne!**
>
> Jeżeli zależy ci na prywatności, nikomu nie podawaj choćby jednej spośród liczb pierwszych p oraz q ani wartości funkcji Eulera. Wykładnik publiczny jest powszechnie znany, więc gdy ktoś pozna również wartość φ(n), może poznać klucz prywatny i złamać szyfr.

Dlaczego p i q muszą być liczbami pierwszymi?

Bezpieczeństwo szyfrowania RSA opiera się na trudności faktoryzacji liczb. Faktoryzacja liczby będącej iloczynem liczb pierwszych, jest bardziej złożona niż faktoryzacja liczb będących iloczynem liczb złożonych. Stąd też p i q muszą być pierwsze.

> **Definicja: funkcja Eulera**
>
> Funkcja Eulera φ(n) to funkcja przypisująca każdej liczbie naturalnej liczbę liczb względnie pierwszych z nią i nie większych od niej.

Drugim powodem tego stanu rzeczy, jest to, że dla liczb pierwszych funkcja Eulera przyjmie następującą postać:

$$\varphi(n) \;=\; \varphi(p \cdot q) \;=\; \varphi(p) \cdot \varphi(q) \;=\; (p-1) \cdot (q-1)$$

Korzystamy tu z następującej właściwości funkcji Eulera:

Jeśli x jest liczbą pierwszą to:

$$\varphi\left(x^k\right) \;=\; x^{k-1} \cdot (x-1)$$

– gdzie p i q to liczby pierwsze o wykładniku równym 1.
Gdyby p i q nie byłyby liczbami pierwszymi, to funkcja Eulera przyjęłaby dużo bardziej złożoną postać, przez co obliczenie jej stałoby się obiektywnie trudniejsze, co w praktycznych zastosowaniach byłoby niekorzystne. Jest to jednak powód drugorzędny.

Załóżmy, że chcemy poznać czyjś klucz prywatny. Klucz publiczny tej osoby jest znany i przyjmuje np. takie wartości: `e = 3` i `n = 33`. Z racji tego, że `n` jest niewielkie, możemy bez większego problemu – przy użyciu tzw. metody brutalnej (siłowej) – ustalić, że `p = 11` i `q = 3`. Tutaj należy zwrócić uwagę, że nie istnieje inna niż 11 i 3 kombinacja liczb, która po pomnożeniu dałaby wynik 33.

Przyjmijmy, że `n = 2501`. Istnieje tylko jedna kombinacja liczb, których iloczyn wynosi dokładnie tyle, ponieważ zmienne `p` i `q` są liczbami pierwszymi. Próba odnalezienia czynników pierwszych metodą brutalną w przypadku n = 2501 jest już bardziej złożona obliczeniowo. Korzystając z niej, musielibyśmy wykonać 40 razy operację dzielenia, zanim odnaleźlibyśmy pierwszy czynnik pierwszy, czyli w tym przypadku `p` równego 41. W tym przykładzie `q` jest równe 61.

> **Ważne!**
>
> Odnalezienie wartości `p` i `q` powinno być w miarę możliwości trudne, dlatego też muszą być one podobnego rzędu, ponieważ nawet jeżeli `n=11485`, to korzystając z metody brutalnej, bardzo szybko otrzymamy czynnik pierwszy `p=5`, a wtedy obliczenie drugiego czynniku nie stanowi już problemu, ponieważ wystarczy podzielić liczbę `n` przez 5.

Dla porównania załóżmy teraz, że `n = 6840`. Liczbę 6840 możemy otrzymać poprzez pomnożenie np. 3420 przez 2, 1710 przez 4, czy też 684 przez 10. Istnieje wiele kombinacji liczb złożonych, dzięki której otrzymalibyśmy wartość takiego `n`.
Reasumując: jeśli `p` i `q` nie są pierwsze, to jesteśmy w stanie rozbić liczbę `n` na wiele czynników pierwszych. Wtedy, pomimo tego, że obliczenie funkcji Eulera staje się potencjalnie dużo bardziej złożone obliczeniowo, to odnalezienie wszystkich czynników pierwszych jest prostsze, a **bezpieczeństwo samego szyfrowania opiera się właśnie na trudności rozkładu liczby `n` na czynniki pierwsze**. Gdy `p` i `q` nie są pierwsze, to możemy skorzystać z innego wzoru na obliczanie funkcji Eulera, a mianowicie:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

- gdzie p_1, p_2, ..., p_k są czynnikami pierwszymi bez powtórzeń.
Przykładowo, dla liczby 32 jedynym czynnikiem pierwszym byłoby 2, podobnie jak dla liczby 1024 lub 8192. Wtedy:

$$\varphi(8192) = 8192(1-\frac{1}{2}) = 4096$$

Jeżeli próbowalibyśmy metodą brutalną odnaleźć wszystkie czynniki pierwsze liczby 8192, to odnaleźlibyśmy je bardzo szybko, ponieważ mimo tego, że liczba ta jest większa niż 2501, dużo prościej się rozkłada.

W przypadku liczb będących iloczynem liczb złożonych jesteśmy w stanie dużo szybciej znaleźć wszystkie czynniki pierwsze metodą brutalną. Aby odnaleźć czynnik pierwszy liczby będącej iloczynem dwóch liczb pierwszych metodą brutalną, musimy w praktyce przeszukać dużo więcej liczb, ponieważ w jej przypadku są tylko dwa czynniki pierwsze.

Jeśli wejdziemy w posiadanie czynników pierwszych, będziemy mogli obliczyć funkcję Eulera, a następnie na tej podstawie będziemy w stanie obliczyć odwrotność modulo `e` liczby `φ(n)`. Wtedy też nasz klucz zostałby złamany.

> **Ważne!**
>
> Bezpieczeństwo RSA opiera się na trudności faktoryzacji liczb. Dlatego też, jak zostało wyjaśnione, `p` i `q` muszą być liczbami pierwszymi podobnego (i możliwie dużego) rzędu, aby trudność ta była jak największa.

Aby obliczyć odwrotność modulo, również należy posługiwać się liczbami pierwszymi.

Odwrotność modulo

> **Definicja: odwrotność modularna**
>
> Odwrotność modularna to operacja polegająca na odnalezieniu dla dowolnej pary $a \; mod \; b$ takiego x, że $a \cdot x \; mod \; b = 1$.
>
> Alternatywnie możemy to zapisać jako $x = a^{-1} \; mod \; b$.

Obliczenie odwrotności modulo można przeprowadzić na wiele sposobów, ale żaden z nich nie ma złożoności wielomianowej. Najprostszą metodą jest metoda naiwna polegająca na podstawianiu pod `x` kolejnych wartości, dopóki nie uzyska się poprawnego wyniku.

Dobrym wyborem jest skorzystanie z rozszerzonego algorytmu Euklidesa.

> **Ważne!**
>
> Rozszerzona wersja algorytmu Euklidesa pozwala odnaleźć kombinację liniową liczb, zgodnie z następującym wzorem:
>
> $$a \cdot x + b \cdot y = NWD(a, b)$$
>
> - gdzie liczba `x` jest odwrotnością modulo `b` liczby `a`, pod warunkiem, że liczby `a` i `b` są względnie pierwsze. Jest to wspomniana wcześniej zależność mówiąca o tym, że aby obliczyć odwrotność modulo, należy operować na liczbach względnie pierwszych, ponieważ tylko liczby względnie pierwsze mają odwrotność modularną.

Załóżmy, że chcemy obliczyć odwrotność modulo 5 liczby 2. W tym celu musimy więc rozwiązać następujące działanie:

$$2 \cdot x \, mod \, 5 \; = \; 1$$

Następnie należy odnaleźć x.

Przeprowadzimy to przy użyciu metody brutalnej:
2 · 1, czyli 2 modulo 5 = 2
2 · 2, czyli 4 modulo 5 = 4
2 · 3, czyli 6 modulo 5 = 1

Zatem pod x możemy wstawić 3.

Nie jest to jednak jedyne rozwiązanie – próbując dalej, będziemy odnajdywać kolejne możliwe wartości x :
2 · 4, czyli 8 modulo 5 = 3
2 · 5, czyli 10 modulo 5 = 0
2 · 6, czyli 12 modulo 5 = 2
2 · 7, czyli 14 modulo 5 = 4
2 · 8, czyli 16 modulo 5 = 1

Zatem pod x można również podstawić 8.

Czy wybór składnika d w kluczu prywatnym ma znaczenie?

Udowodniliśmy, że modulo 5 liczby 2 ma co najmniej dwa rozwiązania – prawda jest jednak taka, że rozwiązań tych jest nieskończenie wiele. Czy istnieje jednak najlepszy wybór wyniku dla klucza prywatnego?

Zaprezentowane wyżej szyfrowanie ma następującą postać:

$$f\left(W\right) = W^{e} mod \, n$$

a z kolei deszyfrowanie będzie miało taką postać:

$$f^{-1}\left(S\right) = S^{d} \, mod \, n$$

> **Przykład 1**
>
> Przyjmijmy następujące dwie liczby pierwsze:
> p = 3
> q = 5
> Zatem:
> n = 3 • 5 = 15

$$\varphi(n) = \varphi(15) = \varphi(3 \cdot 5) = (3-1) \cdot (5-1) \ = \ 2 \ \cdot \ 4 \ = \ 8$$

Wybieramy liczbę względnie pierwszą z przedziału (1, 8).
Może to być chociażby liczba 3, więc przyjmijmy `e = 3`.
Następnie obliczamy odwrotność modulo `φ(n)` liczby `e`, czyli:
`e • x mod φ(n) = 1`, co z kolei po podstawieniu wartości liczbowej daje nam:
3 • x mod 8 = 1.

Z racji tego, że liczby są małe, możemy skorzystać z metody brutalnej:
(3 • 1) mod 8 = 3
(3 • 2) mod 8 = 6
(3 • 3) mod 8 = 1
(3 • 4) mod 8 = 4
(3 • 5) mod 8 = 7
(3 • 6) mod 8 = 2
(3 • 7) mod 8 = 5
(3 • 8) mod 8 = 0
(3 • 9) mod 8 = 3
(3 • 10) mod 8 = 6
(3 • 11) mod 8 = 1

Odwrotnością modulo 8 liczby 3 będzie więc m.in. 3 i 11.
Wartość 3 lub 11 jest też naszą wartością `d` w kluczu prywatnym.

Liczba, którą chcemy zaszyfrować, musi być mniejsza od `n`, które w naszym wypadku wynosi 15. Wybierzmy więc liczbę 13.

$$f\,(13) = 13^3 mod\ 15 \ = \ 2197\ mod\ 15 \ = \ 7$$

Teraz odszyfrujmy wiadomość, korzystając po kolei z 3 i 11 jako wartości `d`.

$$f^{-1}(7) = 7^3\ mod\ 15 \ = 343\ mod\ 15 \ = \ 13$$

$$f^{-1}(7) = 7^{11}\ mod\ 15 \ = 1977326743\ mod\ 15 \ = \ 13$$

Na zaprezentowanym powyżej przykładzie widać, że dla poprawności algorytmu nie ma znaczenia, jaką liczbę wybierzemy jako `d`, dopóki będzie ona odwrotnością modulo `φ(n)` liczby `e`. Z obliczeniowego punktu widzenia najkorzystniejszą decyzją jest wybranie mniejszego `d`, jednakże `d` nie powinno być równe `e`. Należy unikać sytuacji,

w których klucz prywatny i klucz publiczny posiada takie same wartości, ponieważ byłaby to słabość, która mogłaby zostać wykorzystana przez naszego potencjalnego przeciwnika. W tym przypadku najlepszym wyborem, ze względu na bezpieczeństwo, byłoby więc wybranie d równego 11.

Dlaczego szyfrowanie i deszyfrowanie działa?

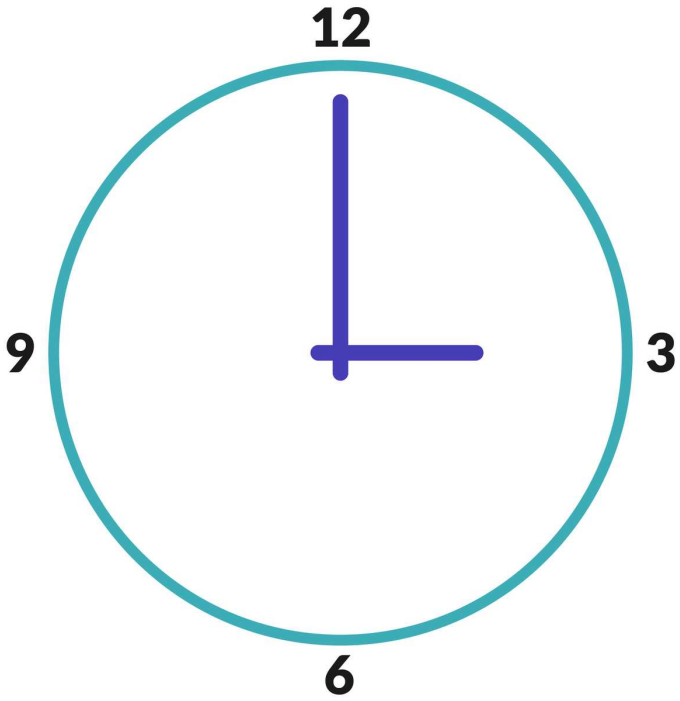
Poniższa funkcja:

$$f(W) = W^e mod\, n$$

oraz funkcja odwrotna:

$$f^{-1}(S) = S^d\ mod\, n$$

służą kolejno do szyfrowania i deszyfrowania, a zasada ich działania opiera się na arytmetyce modularnej, którą można wyjaśnić na przykładzie zegara.



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

Zegar wskazuje godzinę trzecią – dla przykładu załóżmy, że interesuje nas jedynie zachowanie wskazówki godzinowej. Mija 12 godzin – zegar ponownie wskazuje godzinę trzecią. Czy czas stanął w miejscu? Czy jest to ta sama godzina trzecia, co 12 godzin temu? Oczywiście, że nie.

Stwierdzenie więc, że 3 + 12 = 3 jest niepoprawne, ponieważ godziny te nie są sobie równe, lecz są do siebie **przystające**. W matematyce operację przystawania zapisujemy tak:

$$a \equiv_n b$$

Możemy też zapisać tę relację w nastepujący sposób:

$$[a]_n = [b]_n$$

> **Definicja: przystawanie**
>
> Przystawanie (inaczej: kongruencja) modulo `n` to sytuacja, w której reszty z dzielenia a i b przez n są równe (wówczas zachodzi równanie: `a % n = b % n`, co można zapisać też jako `[a]n = [b]n`).

Przedstawiona wcześniej reguła z zegarem matematycznie prezentowałaby się więc tak:

$$[3 + 12]_{12} = [3]_{12}$$

Operacja szyfrowania i deszyfrowania opiera się na następującej zasadzie:

$$[a^e]_n = \left[([a^e]_n)^d\right]_n$$

Dlatego też wysyłana przez nas wiadomość w postaci liczbowej musi być mniejsza od `n`, ponieważ wtedy nawet dla `e = 1` i `d = 1` wiadomość, którą chcemy wysłać, byłaby różna od tej, którą finalnie otrzymamy.

> **Dla zainteresowanych**
>
> Jeśli interesuje cię temat nietypowej arytmetyki, w której 12 + 3 może być równe 3, warto zapoznać się z pojęciem struktury algebraicznej, a przede wszystkim grupy oraz pierścienia.

Teoria a praktyka

Im większe liczby pierwsze `p` i `q`, tym trudniej jest odgadnąć choćby jedną z nich. Można tu sobie zadać zasadne pytanie: skoro atakujący wie, że korzystamy jedynie z liczb pierwszych, to czemu nie odnajdzie wszystkich liczb pierwszych i nie sprawdzi po prostu wszystkich kombinacji?

Głównym problemem takiej strategii jest fakt, że liczb pierwszych jest nieskończenie wiele, zatem chcąc przeciwdziałać metodzie brutalnej, powinniśmy za nasze `p` i `q` przyjąć możliwie jak największe liczby pierwsze, które są podobnych rzędów wielkości. Właśnie dlatego w praktycznych zastosowaniach używa się kluczy mających po kilkaset bitów (dla

przypomnienia: liczba mająca 64 bity może mieć maksymalnie wartość 18 446 744 073 709 551 615).

Jak już powiedzieliśmy, liczb pierwszych jest nieskończenie wiele. Największą znaną i potwierdzoną liczbą pierwszą na dzień 21.06.2020 jest liczba składająca się z **22 338 618 cyfr**.

Wzór na oszacowanie liczby liczb pierwszych pomiędzy 0 a `x` to:

$$\frac{x}{\ln x}$$

Błąd dla `x = 50000` wynosi jedynie 0,6% i dla większych wartości tylko się zmniejsza. Czyli liczb pierwszych do liczby 50000 jest około 4621 +/- 0,6%.

Słownik

> **liczba pierwsza**
>
> liczba naturalna większa od 1, mająca tylko dwa dzielniki: 1 oraz siebie samą (przykładowo: 2, 3, 5, 7, 11)
> **liczba złożona**
>
> liczby złożone to liczby naturalne, które posiadają więcej niż dwa dzielniki. (przykładowo: 6, 9, 12, 14)
> **szyfrogram**
>
> zaszyfrowana wiadomość
> **faktoryzacja liczb**
>
> inaczej rozkład na czynniki pierwsze

Prezentacja multimedialna

Polecenie 1

Przeanalizuj krok po kroku proces szyfrowania i deszyfrowania wiadomości za pomocą szyfru RSA, przedstawiony na przykładzie konkretnej sytuacji.

Polecenie 2

Sprawdź się

Pokaż ćwiczenia:

- Ćwiczenie 1
- Ćwiczenie 2
- Ćwiczenie 3
- Ćwiczenie 4
- Ćwiczenie 5
- Ćwiczenie 6
- Ćwiczenie 7
- Ćwiczenie 8
- Ćwiczenie 9
- Ćwiczenie 10
- Ćwiczenie 11
- Ćwiczenie 12
- Ćwiczenie 13
- Ćwiczenie 14

Ćwiczenie 15

Dla nauczyciela

Autor: Maurycy Gast
Przedmiot: Informatyka

Temat: Szyfr RSA

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres 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 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 podstawowe różnice pomiędzy kluczem prywatnym a publicznym.
- Przeanalizujesz mechanizm wyznaczania klucza prywatnego i publicznego w algorytmie RSA.
- Wyjaśnisz, co to jest arytmetyka modularna i jak działa szyfr RSA.

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: „Szyfr RSA". Uczniowie mają zapoznać się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Wyświetlenie przez nauczyciela tematu i celów zajęć, przejście do wspólnego ustalenia kryteriów sukcesu.
2. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu e-materiału. Indywidualnie zapoznają się z treścią w sekcji „Przeczytaj".
2. Nauczyciel wyświetla zawartość sekcji „Przeczytaj". Na forum klasy uczniowie analizują przedstawione w niej treści i rozwiązanie Przykładu 1.
3. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Prezentacja multimedialna". Uczniowie wspólnie analizują krok po kroku proces szyfrowania i deszyfrowania wiadomości za pomocą szyfru RSA przedstawiony na przykładzie konkretnej sytuacji.
4. Uczniowie w parach wykonują ćwiczenia nr 1-8. Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. 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".
2. Wybrany uczeń podsumowuje zajęcia, zwracając uwagę na nabyte umiejętności.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 9-15 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj” można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.