

Ewentualne potrzebne pliki: www.code.kopernik-leszno.pl/zbiorzadan/pliki.zip

Zadanie 78.

Wiązka zadań *Podpis elektroniczny*

Bajtek otrzymał od przyjaciela 11 jawnych wiadomości. Do każdej wiadomości przyjaciel dołączył podpis elektroniczny.

Podpis elektroniczny jest **zaszyfrowanym skrótem** wiadomości. Przyjaciel Bajtka utworzył skrót za pomocą funkcji *skrot()*, która przekształca dowolną wiadomość w 8-znakowy napis, a następnie zaszyfrował ten skrót algorytmem A o sobie tylko znanym kluczu prywatnym (e,n) . Opis obu algorytmów podano poniżej.

Bajtek chciałby być pewien, że zachowano:

- integralność danych (treść nie została zmieniona w trakcie przesyłania),
- uwierzytelnienie nadawcy (nikt się pod nadawcę nie podszył).

W tym celu powinien sprawdzić każdą wiadomość następująco:

- zaprogramować funkcję *skrot(wiadomosc)* i za jej pomocą utworzyć skrót wiadomości,
- odszyfrować skrót z podpisu elektronicznego algorytmem A przy pomocy ogólnie znanego klucza publicznego (d,n) o wartościach **(3,200)**,

- porównać oba skróty: jeśli są identyczne, znaczy to, że wiadomość jest wiarygodna.

Pomóż Bajtkowi sprawdzić, czy otrzymane wiadomości są wiarygodne.

W pliku `wiadomosci.txt` znajduje się 11 wiadomości, każda w osobnym wierszu. Liczba znaków każdej wiadomości nie przekracza 255. Wiadomości zawierają znaki pojedynczego odstępu, które są integralną częścią informacji.

W pliku `podpisy.txt` znajduje się 11 wierszy, każdy z nich zawiera 8 liczb całkowitych, stanowiących elementy podpisu elektronicznego jednej wiadomości. Liczby w wierszu oddzielone są pojedynczymi znakami odstępu. Kolejność wierszy podpisów jest zgodna z kolejnością wierszy wiadomości (pierwszy wiersz podpisów odpowiada pierwszej wiadomości, drugi — drugiej itd.)

Funkcja skrótu *skrot(wiadomość)*

Skrót wiadomości jest 8-znakowym napisem, złożonym z wielkich liter alfabetu angielskiego.

Aby go wyznaczyć, wykonaj następujące kroki:

- Wpisz do 8-elementowej tablicy S kody ASCII znaków słowa "ALGORYTM".
- Treść wiadomości uzupełnij na końcu znakami kropki '.' do wielokrotności 8 znaków.
- Rozpatrz po kolei 8-znakowe porcje treści wiadomości. W zależności od kodów ich znaków aktualizuj wartości elementów w tablicy S . Dla każdej porcji treści wiadomości powtarzaj:

dla $j=1,2 \dots 8$ wykonuj

$$S[j] \leftarrow (S[j] + \text{kod znaku na } j\text{-tej pozycji w bieżącej porcji wiadomości}) \bmod 128$$

- Zbuduj wynik, wyznaczając jego kolejne znaki na podstawie elementów tablicy S :

$\text{wynik} = ""$

dla $j=1,2 \dots 8$ wykonuj

$$\text{wynik} \leftarrow \text{wynik} + \text{char}(65 + S[j] \bmod 26)$$

gdzie: \bmod jest operatorem dzielenia modulo,

funkcja $\text{char}(kod)$ zwraca reprezentację graficzną znaku o podanym kodzie

Otrzymany w ten sposób wynik jest skrótem wiadomości.

Algorytm A szyfrowania z kluczem prywatnym (e,n) i deszyfrowania kluczem publicznym (d,n)

Deszyfrowanie polega na wykonaniu operacji $x=(y*d \bmod n)$, gdzie za y należy przyjąć kolejne liczby tworzące podpis elektroniczny. Tekst wynikowy można otrzymać, składając w jeden napis reprezentacje graficzne kolejnych liczb x zgodnie ze standardem ASCII.

Uwaga dla dociekliwych

Zaszyfrowanie algorytmem A polegało na wykonywaniu operacji $y=(x*e \bmod n)$, gdzie za x należało podstawić kody ASCII kolejnych znaków tekstu źródłowego. Uzyskany w ten sposób ciąg liczb jest podpisem elektronicznym wiadomości. Gdyby ktoś chciał złamać szyfr A , czyli wyznaczyć nieznany element e klucza prywatnego, musiałby znaleźć taką wartość e , względnie pierwszą z d , że $e*d \bmod n = 1$. Uzasadnienia szukaj w prawach arytmetyki modularnej. **Proste? :)**

Napisz program rozwiązujący poniższe zadania. Do oceny oddaj plik tekstowy `epodpis_wynik.txt`, zawierający odpowiedzi, oraz plik (pliki) zawierający reprezentację komputerową Twojego rozwiązania.

78.1.

Wyznacz skrót **pierwszej** wiadomości z pliku `wiadomosci.txt` i udokumentuj wyniki kolejnych etapów obliczania tego skrótu. Zapisz w kolejnych wierszach pliku wynikowego:

- liczbę znaków wiadomości po jej uzupełnieniu do najmniejszej długości o wielokrotności 8 znaków,
- wartości liczbowe 8 kolejnych bajtów skrótu (elementy tablicy S) po przetworzeniu całej wiadomości — wszystkie wartości w jednym wierszu, oddzielone pojedynczymi znakami odstępu,
- skrót wiadomości w postaci napisu o długości 8, złożonego z wielkich liter alfabetu angielskiego.

78.2.

Odszyfruj skróty wiadomości ze wszystkich podpisów elektronicznych umieszczonych w pliku `podpisy.txt`, stosując algorytm A z kluczem publicznym $(d, n) = (3, 200)$. Zapisz uzyskane skróty w kolejnych, osobnych wierszach pliku z odpowiedziami.

78.3.

Zweryfikuj wiarygodność wszystkich wiadomości i podaj numery wiadomości wiarygodnych. Zapisz w jednym wierszu pliku z odpowiedziami, jako liczby z zakresu 1..11, zgodnie z kolejnością umieszczenia ich w pliku danych, oddzielone pojedynczym znakiem odstępu.

Publikacja opracowana przez zespół koordynowany przez **Renatę Świrko** działający w ramach projektu *Budowa banków zadań* realizowanego przez Centralną Komisję Egzaminacyjną pod kierunkiem Janiny Grzegorek.

Autorzy

dr Lech Duraj
dr Ewa Kołczyk
Agata Kordas-Łata
dr Beata Laszkiewicz
Michał Malarski
dr Rafał Nowak
Rita Pluta
Dorota Roman-Jurdzińska

Komentatorzy

prof. dr hab. Krzysztof Diks
prof. dr hab. Krzysztof Loryś
Romualda Laskowska
Joanna Śmigielska

Opracowanie redakcyjne

Jakub Pochrybniak

Redaktor naczelny

Julia Konkołowicz-Pniewska

Zbiory zadań opracowano w ramach projektu *Budowa banków zadań*,
Działanie 3.2 Rozwój systemu egzaminów zewnętrznych,
Priorytet III Wysoka jakość systemu oświaty,
Program Operacyjny Kapitał Ludzki