Test

Bezpieczeństwo WWW

1. Szyfrowanie danych, z użyciem algorytmów kryptografii symetrycznej, przesyłanych przez Internet nie zapewnia:
a) poufności (tajności) danych,
b) spójności (integralności) danych,
c) wiarygodności (potwierdzenia autentyczności) danych,
d) więcej niż jedna z powyższych odpowiedzi jest prawdziwa.

2. Przykładem szyfru przedstawieniowego jest:
a) metoda płotu,
b) szyfr Cezara,
c) szyfr Vigenère'a,
d) żadna z powyższych odpowiedzi nie jest prawdziwa.

3. Zasada mówiąca, że system kryptograficzny powinien być bezpieczny nawet wtedy, gdy wszystkie szczegóły jego działania – oprócz klucza – są znane to zasada:
a) Vigenère'a,
b) Babbage'a,
c) Turinga,
d) Kerckhoffsa.

4. Asymetryczny system kryptograficzny charakteryzuje:
a) łatwość generowania podpisu cyfrowego,
b) duża szybkość szyfrowania i deszyfrowania,
c) duża szybkość generowania i weryfikowania znacznika MAC,
d) wszystkimi wyżej wymienionymi cechami.

5. Przykładem współczesnej metody szyfrowania symetrycznego jest algorytm o nazwie:
a) RSA
b) MAC
c) RC4
d) wszystkie wyżej wymienione algorytmy to przykłady systemów asymetrycznych.

6. Liczby, które mają tylko dwa dzielniki właściwe nazywa się:
a) pierwszymi,
b) półpierwszymi,
c) pseudopierwszymi,
d) quasi-pierwszymi.

7. Idea szybkiego podnoszenia do potęgi jest wykorzystywany w realizacji algorytmu:
a) Euklidesa,
b) rozkładu na czynniki pierwsze (faktoryzacji),
c) RSA,
d) w każdym z wyżej wymienionych algorytmów.

8. W realizacji algorytmu RSA stosuje się algorytm:
a) algorytmu badania pierwszości liczby,
b) algorytm Euklidesa,
c) algorytm szybkiego podnoszenia do potęgi,
d) wszystkie z powyższych odpowiedzi są poprawne.

9. Bezpieczeństwo systemu asymetrycznego RSA opiera się na trudności:
a) badania pierwszości bardzo wielkiej liczby,
b) rozkładu bardzo wielkiej liczby na czynniki pierwsze,
c) obliczenia logarytmu w arytmetyce modularnej,
d) przynajmniej dwie z powyższych odpowiedzi są poprawne.

10. Do etapów procesu realizacji podpisu cyfrowego nie należy:
a) tworzenie tzw. skrótu wiadomości, która ma być podpisana,
b) szyfrowanie ww. skrótu kluczem prywatnym twórcy wiadomości,
c) tworzenie tzw. skrótu odebranej wiadomości przez odbiorcę,
d) wszystkie z powyższych odpowiedzi są poprawne.