**KRYPTOLOGIA**

**EGZAMIN I TERMIN**

1. **Wklejamy tu treść pytania, jeśli pytanie się powtarza usuwamy drugie takie same.kryptologia to nauka obejmująca kryptografię i kryptoanalizę,**

****

1. **Kolorem Zielonym zaznaczamy tą odpowiedź której jesteśmy PEWNI**
2. **Kolorem Żółtym zaznaczamy odpowiedź która może być prawidłowa ale nie jesteśmy pewni**
3. **Kolorem czerwonym zaznaczamy odpowiedź która NA PEWNO jest nieprawidłowa.**
4. **Na ten plik wchodzimy za pomocą trybu incognito wtedy jesteśmy anonimowo podpisani**

**seks z szyframi seks z szyframi**

**kryptogej**

1

**W celu zapewnienia bezpieczeństwa kryptograficznego:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **urządzenie/oprogramowanie kryptograficzne powinno być właściwie eksploatowane,**
* **algorytm kryptograficzny powinien być poprawnie zaprojektowany,**
* **eksploatacja urządzenia kryptograficznego nie ma wpływu na bezpieczeństwo kryptograficzne,**
* **algorytm kryptograficzny powinien być poprawnie zaimplementowany,**

2

**Podstawowe atrybuty kryptograficznej ochrony informacji to:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **dostępność,**
* **poufność,**
* **uwierzytelnienie,**
* **integralność,**

3

**Kryptograficzna usługa poufności ma na celu:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **zapewnienie dostępności danych,**
* **ochronę danych przed ich ujawnieniem,**
* **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane),**
* **potwierdzenie tożsamości danej strony protokołu kryptograficznego,**

**Kryptograficzna usługa integralności ma na celu:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **potwierdzenie tożsamości danej strony protokołu kryptograficznego,**
* **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane),**
* **ochronę danych przed ich ujawnieniem,**
* **zapewnienie dostępności danych,**

5

**Kryptograficzna usługa uwierzytelnienia ma na celu:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane),**
* **potwierdzenie tożsamości danej strony protokołu kryptograficznego,**
* **zapewnienie dostępności danych,**
* **ochronę danych przed ich ujawnieniem,K**

6

**System kryptograficzny zapewniający poufność informacji musi spełniać następujące warunki:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **przekształcenia szyfrujące i deszyfrujące muszą być efektywne dla wszystkich kluczy,**
* **nie może zawierać mechanizmów pozwalających na odczyt informacji przez nieuprawnione strony protokołu kryptograficznego, tzw. tylne furtki (back doors),**
* **przekształcenia szyfrujące i deszyfrujące muszą być wzajemnie odwrotne,**
* **może zawierać mechanizmy pozwalające na odczyt informacji przez nieuprawnione strony protokołu kryptograficznego tzw. tylne furki (back doors),**

**Zasada Kerckhoffsa stwierdza, że:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **bezpieczeństwo kryptosystemu powinno być oparte na tajności odpowiednich kluczy kryptograficznych i nie zależeć od tajności algorytmów kryptograficznych,**
* **bezpieczeństwo kryptosystemu powinno być oparte na tajności odpowiednich kluczy kryptograficznych oraz zależeć od tajności algorytmów kryptograficznych,**
* **bezpieczeństwo kryptosystemu powinno być oparte na jawności wszystkich kluczy kryptograficznych oraz zależeć od tajności algorytmów kryptograficznych,**
* **bezpieczeństwo kryptosystemu powinno być oparte na jawności wszystkich kluczy kryptograficznych i nie zależeć od tajności algorytmów kryptograficznych,**

8

**W kryptografii symetrycznej:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **każda ze stron protokołu kryptograficznego posiada 2 różne klucze: publiczny (jawny) oraz prywatny (tajny),**
* **w procesie szyfrowania deszyfrowania wykorzystują szyfry blokowe i/lub strumieniowe,**
* **w procesie szyfrowania/deszyfrowania używany jest ten sam klucz kryptograficzny,**
* **zapewniają uwierzytelnienie poprzez generację/wertyfikację podpisu cyfrowego,**

**Chat:**

* + **W procesie szyfrowania/deszyfrowania wykorzystują szyfry blokowe i/lub strumieniowe.**
  + **W procesie szyfrowania/deszyfrowania używany jest ten sam klucz kryptograficzny.szyfr**

**W kryptografii symetrycznej klucze powinny spełniać następujące warunki:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **klucz szyfrowania może być jawny, natomiast klucz deszyfrowania musi być tajny,**
* **klucz szyfrowania/deszyfrowania musi być tajny,**
* **klucz szyfrowania/deszyfrowania może być jawny,**
* **klucz deszyfrowania może być jawny, natomiast klucz szyfrowania musi być tajny,**

10

**Kryptograficzna funkcja skrótu:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **służy do realizacji usługi poufności informacji,**
* **służy do realizacji usługi integralności informacji,**
* **przekształca ciąg binarny o dowolnej, skończonej długości w wektor binarny o określonej długości,**
* **przekształca ciąg binarny o określonej długości w ciąg bitów o tej samej długości,**

**Szyfry blokowe:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego za pomocą tajnego klucza symetrycznego,**
* **stanowią klasę kryptosystemów symetrycznych,**
* **stanowią klasę kryptosystemów asymetrycznych,**
* **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego za pomocą jawnego klucza asymetrycznego,**

**Szyfry strumieniowe:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego za pomocą tajnego klucza symetrycznego.**
* **stanowią klasę kryptosystemów asymetrycznych,**
* **przekształcają strumień bitów tekstu jawnego w strumień bitów tekstu zaszyfrowanego za pomocą strumienia bitów tajnego klucza symetrycznego,**
* **stanowią klasę kryptosystemów symetrycznych,**

13

**Współczesne szyfry strumieniowe mogą być projektowane w oparciu o:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **architekturę Feistela,**
* **nieliniowe rejestry ze sprzężeniem zwrotnym NFSR, (mogą być)**
* **architekturę sieci podstawieniowo-przestawieniowej SPN,**
* **liniowe rejestry ze sprzężeniem zwrotnym LFSR,**

**chat:**

* **Nieliniowe rejestry ze sprzężeniem zwrotnym NFSR.**
* **Liniowe rejestry ze sprzężeniem zwrotnym LFSR.**

**Współczesne szyfr blokowe mogą być projektowane w oparciu o:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **architekturę sieci Feistela,**
* **rejestry z liniowym sprzężeniem zwrotnym LFSR,**
* **strukturę iteracyjną Merklego-Damgarda MD,**
* **architekturę sieci podstawieniowo-przestawieniowej SPN,**

**Funkcja skrótu może być zbudowana w oparciu o strukturę:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **gąbki,**
* **LFSR,**
* **sieć Feistela**
* **Merkle-Damgarda,**

**AES:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **jest standardem szyfrowania blokowego,**
* **długość klucza wynosi 128, 192 lub 256 bitów,**
* **zastosowano konstrukcję sieci Feistela,**
* **zastosowano konstrukcję sieci podstawieniowo-przestawieniowej SPN,**

**Funkcja skrótu SHA – 3:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **jest standardem funkcji skrótu,**
* **daje skrót o długości 224, 256, 384 lub 512 bitów,**
* **zbudowana jest w oparciu o architekturę "gąbki" (sponge construction),**
* **zbudowana jest w oparciu o konstrukcję Merkle-Damgarda (MD),**

**W kryptografii asymetrycznej:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **klucze asymetryczne publiczny i prywatny są wygenerowane losowo i nie zależą od siebie,**
* **klucze asymetryczne publiczny i prywatny są wygenerowane z wykorzystaniem problemu trudno obliczeniowego i są wzajemnie zależne,**
* **każda strona protokołu kryptograficznego posiada parę kluczy asymetrycznych: publiczny (jawny) i prywatny (tajny),**
* **każda strona protokołu kryptograficznego posiada wspólny klucz tajny,**

**Kryptosystemy asymetryczne:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **bezpieczeństwo zależy od aktualnej wiedzy i możliwości technologicznych dot. rozwiązywania danego problemu trudnoobliczeniowego,**
* **bezpieczeństwo oparte jest na problemie trudnym obliczeniowo,**
* **są warunkowo bezpieczne,**
* **są bezwarunkowo bezpieczne,**

**Protokół Diffie-Hellmana służy do:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **ustalenia wspólnej, tajnej wartości, która może służyć do generacji klucza symetrycznego przez strony protokołu kryptograficznego,**
* **generacji/weryfikacji podpisu cyfrowego wiadomości,**
* **uwierzytelniania wiadomości,**
* **szyfrowania/deszyfrowania wiadomości,**

**Nadawca chce wysłać do Odbiorcy wiadomość podpisaną cyfrowo . Którego klucza użyje Nadawca w procesie generacji podpisu cyfrowego?**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **klucza publicznego Nadawcy,**
* **klucza prywatnego Nadawcy,**
* **klucza publicznego Odbiorcy,**
* **klucza prywatnego Odbiorcy,**

**Nadawca chce wysłać do Odbiorcy wiadomość zaszyfrowaną przy użyciu kryptosystemu asymetrycznego. Którego klucza użyje Nadawca w procesie szyfrowania?**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **klucza prywatnego Odbiorcy,**
* **klucza prywatnego Nadawcy,**
* **klucza publicznego Odbiorcy,**
* **klucza publicznego Nadawcy,**

**W kryptografii asymetrycznej, w przypadku wiadomości nadawanej przez Nadawcę i odbieranej przez Odbiorcę:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **w realizacji usługi poufności wiadomości klucz publiczny Odbiorcy służy do szyfrowania wiadomości przez nadawcę, a klucz prywatny Odbiorcy do jej deszyfrowania przez odbiorcę,**
* **w realizacji usługi poufności wiadomości, klucz prywatny Nadawcy służy do szyfrowania wiadomości, a klucz publiczny Odbiorcy do jej deszyfrowania przez odbiorcę,**
* **w realizacji usługi uwierzytelnienia nadawcy klucz prywatny Nadawcy służy do generacji podpisu cyfrowego a klucz publiczny Nadawcy do jego weryfikacji przez odbiorcę,**
* **w realizacji usługi uwierzytelnienia nadawcy klucz prywatny Odbiorcy służy do generacji podpisu cyfrowego a klucz publiczny Odbiorcy do jego weryfikacji przez odbiorcę,**

**chat:**

* **W realizacji usługi poufności wiadomości klucz publiczny Odbiorcy służy do szyfrowania wiadomości przez nadawcę, a klucz prywatny Odbiorcy do jej deszyfrowania przez odbiorcę.**
* **W realizacji usługi uwierzytelnienia nadawcy klucz prywatny Nadawcy służy do generacji podpisu cyfrowego a klucz publiczny Nadawcy do jego weryfikacji przez odbiorcę.**

**elgamalKryptograficzna usługa uwierzytelnienia ma na celu:**

**Kryptosystem RSA może służyć do:**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **zapewnienia dostępności do wiadomości,**
* **generacji/weryfikacji podpisu cyfrowego wiadomości,**
* **szyfrowania/deszyfrowania wiadomości,**
* **zapewnienia integralności wiadomości,**

**Bezpieczeństwo protokołu Diffie-Hellmana oparte jest na:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **problemie obliczania logarytmu dyskretnego w ciele punktów na krzywej eliptycznej,**
* **problemie obliczania logarytmu dyskretnego w ciele liczb skończonych modulo duża liczba pierwsza,**
* **problemie wyznaczania punktów krzywej eliptycznej,**
* **problemie faktoryzacji (rozkładzie na czynniki pierwsze) dużej liczby złożonej,**

**chat:**

**Problemie obliczania logarytmu dyskretnego w ciele liczb skończonych modulo duża liczba pierwsza.**

**Problemem trudno obliczeniowym dla algorytmu ElGamala jest:**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **problem obliczania logarytmu dyskretnego na krzywych eliptycznych,**
* **problem plecakowy,**
* **problem faktoryzacji (rozkład liczby złożonej na czynniki pierwsze),**
* **problem obliczania logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza,**

**chat:**

**Problem obliczania logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza.**

**Obecnie minimalna (rekomendowana przez NIST) długość klucza RSA wynosi:**

**Wybierz 1 z 4 odpowiedzi:**

* **512 bitów,**
* **1024 bity,**
* **2048 bity,**
* **4096 bitów,**

**chat:**

**2048 bitów.**

**Obecnie, minimalna (rekomendowana przez NIST) długość klucza ElGamala wynosi:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **512 bitów**
* **1024 bity**
* **2048 bity**
* **4096 bitów**
* **chat: 2048 bitów.**

**Które z poniższych sformułowań jest prawdziwe?**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **kryptologia to nauka obejmująca kryptografię i kryptoanalizę,**
* **kryptoanaliza to dziedzina wiedzy i badań zajmująca się analizowaniem (łamaniem) istniejących algorytmów kryptograficznych,**
* **kryptologia zajmuje się ukrywaniem informacji,**
* **kryptografia to dziedzina wiedzy i badań zajmująca się tworzeniem nowych algorytmów kryptograficznych,**

**Które z poniższych sformułowań jest prawdziwe?**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **kryptologia zajmuje się ukrywaniem informacji,**
* **kryptografia to dziedzina wiedzy i badań zajmująca się tworzeniem nowych algorytmów kryptograficznych,**
* **kryptologia to nauka obejmująca kryptografię i kryptoanalizę,**
* **kryptoanaliza to dziedzina wiedzy i badań zajmująca się analizowaniem (łamaniem) istniejących algorytmów kryptograficznych,**

**Wszystkie cztery sformułowania są prawdziwe. Kryptologia zajmuje się ukrywaniem informacji, kryptografia to dziedzina wiedzy i badań zajmująca się tworzeniem nowych algorytmów kryptograficznych, kryptologia to nauka obejmująca kryptografię i kryptoanalizę, a kryptoanaliza to dziedzina wiedzy i badań zajmująca się analizowaniem (łamaniem) istniejących algorytmów kryptograficznych. Czy chcesz dowiedzieć się więcej na ten temat?**

**Trivium:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **zbudowany został na bazie rejestru z liniowym sprzężeniem zwrotnym LFSR,**
* **długość klucza oraz długość wektora IV wynosi po 80 bitów ,**
* **jest standardem szyfrowania strumieniowego,**
* **zbudowany został na bazie 3 rejestrów przesuwnych,**

**Kryptosystem ElGamala może służyć do:**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **zapewnienia integralności wiadomości,**
* **generacji/weryfikacji podpisu cyfrowego wiadomości,**
* **szyfrowania/deszyfrowania wiadomości,**
* **zapewnienia dostępności do wiadomości,**

**Odbiorca otrzymał od Nadawcy wiadomość zaszyfrowaną przy użyciu kryptosystemu asymetrycznego. Którego klucza użyje Odbiorca w procesie deszyfrowania?**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **klucza prywatnego Odbiorcy,**
* **klucza prywatnego Nadawcy,**
* **klucza publicznego Odbiorcy,**
* **klucza publicznego Nadawcy,**

**Problemem trudno obliczeniowym dla RSA jest:**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **problem obliczania logarytmu dyskretnego w ciele liczb całkowitych modulo liczba pierwsza,**
* **problem obliczania logarytmu dyskretnego na krzywych eliptycznych,**
* **problem plecakowy,**
* **problem faktoryzacji (rozkład liczby złożonej na czynniki pierwsze),**

**Odbiorca otrzymał od Nadawcy wiadomość podpisaną cyfrowo przy użyciu kryptosystemu asymetrycznego. Którego klucza użyje Odbiorca w procesie weryfikacji otrzymanego podpisu cyfrowego?**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **klucza prywatnego Nadawcy,**
* **klucza publicznego Odbiorcy,**
* **klucza prywatnego Odbiorcy,**
* **klucza publicznego Nadawcy,**

**Problemem trudno obliczeniowym dla RSA jest:**

**Wybierz od 1 do 4 poprawnych odpowiedzi.**

* **problem faktoryzacji (rozkład liczby złożonej na czynniki pierwsze),**
* **problem obliczania logarytmu dyskretnego w ciele liczb całkowitych modulo liczba pierwsza,**
* **problem obliczania logarytmu dyskretnego na krzywych eliptycznych,**
* **problem plecakowy,**

23

**W kryptografii asymetrycznej, w przypadku wiadomości nadawanej przez Nadawcę i odbieranej przez Odbiorcę:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **w realizacji usługi poufności wiadomości klucz publiczny Odbiorcy służy do szyfrowania wiadomości przez nadawcę, a klucz prywatny Odbiorcy do jej deszyfrowania przez odbiorcę,**
* **w realizacji usługi poufności wiadomości, klucz prywatny Nadawcy służy do szyfrowania wiadomości, a klucz prywatny Odbiorcy do jej deszyfrowania przez odbiorcę,**
* **w realizacji usługi uwierzytelnienia nadawcy klucz prywatny Nadawcy służy do generacji podpisu cyfrowego a klucz publiczny Nadawcy do jego weryfikacji przez odbiorcę,**
* **w realizacji usługi uwierzytelnienia nadawcy klucz publiczny Odbiorcy służy do generacji podpisu cyfrowego a klucz prywatny Odbiorcy do jego weryfikacji przez odbiorcę,**

**Obecnie minimalna (wg NIST) długość liczby pierwszej w protokole Diffie-Hellmana, zapewniająca bezpieczeństwo kryptograficzne wynosi:**

**Wybierz od 1 do 4 poprawnych odpowiedzi:**

* **512 bitów,**
* **1024 bity,**
* **2048 bitów,**
* **4096 bitów.**