1. Co oznacza że System Informatyczny (SI) jest systemem bezpiecznym?

Definicja:
System informatyczny jest bezpieczny, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.
SI jest systemem bezpiecznym, gdy:

- gwarantuje poufność oraz integralność danych;
- ogranicza dostępność osobom, obiektom, oprogramowaniu nieuprawnionemu;
- zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją;
- użytkownik może na nim polegać (jest bezpieczny do korzystania).

2. Jakie znasz kryteria oceny systemów informatycznych?

Poufność – ochrona przed ujawnieniem informacji
Integralność – ochrona przed modyfikacją
Dostępność – gwarancja uprawnionego dostępu
Rozliczalność – określenie i weryfikacja odpowiedzialności
Autentyczność – weryfikacja tożsamości (zapewnione uwierzytelnianie)
Niezawodność – gwarancja odpowiedniego zachowania się systemu

3. Jakie znasz środki utrzymania bezpieczeństwa?

Fizyczne – ochrona strefy bezpieczeństwa (zamki, kraty, kable) ochrona przed żywiołami, ochrona przed promieniowaniem elektromagnetycznym, ochrona nośników danych
Techniczne – kryptografia, kontrola dostępu do zasobów SI, ochrona przed awariami zasilania, ochrona antywirusowa, VPN, macierze RAID i systemy backupu.
Prawne – wszelkie wymagania, które nakłada prawo (standardy)
Organizacyjno-administracyjne – szkolenia, ograniczenia

4. Jakie znasz klasyfikacje systemów kryptograficznych?

Podział ze względu na ***klucza kryptograficznego***:
Kryptografia symetryczna – Nadawca i odbiorca mają ten sam klucz
Kryptografia asymetryczna – Występuje tu klucz publiczny i prywatny, wiadomość zaszyfrowana kluczem publicznym, może być odczytana tylko przy użyciu klucza prywatnego.

Podział ze względu na ***bezpieczeństwo***:
Bezpieczeństwo bezwarunkowe
– Niezależnie od ilości przechwyconego tekstu zaszyfrowanego, nie ma w nim wystarczająco dużo informacji aby jednoznacznie określić tekst jawny
– Korzystanie z jednorazowych kluczy
Bezpieczeństwo obliczeniowe
– Szyfru nie można złamać przy zastosowaniu systematycznej analizy z użyciem dostępnych zasobów
– Stosowane obecnie najczęściej, bo nie można go złamać w krótkim czasie

5. Podaj różnice pomiędzy kryptografią asymetryczną a symetryczną?

Kryptografia symetryczna	Kryptografia asymetryczna
Mniej wymagająca obliczeniowo	Bardziej skomplikowana
Szybsza	Bardziej wymagająca, wolniejsza
Do szyfrowania i odszyfrowania wykorzystywany jest 1 klucz	2 różne klucze potrzebne do szyfrowania i odszyfrowania
Przeważnie wykorzystywana do szyfrowania dużych partii danych	Przeważnie wykorzystywana do szyfrowania kluczy
Proste klucze	Rozbudowane klucze
Przykład: AES, DES	Przykład: RSA

6. Systematyka szyfrów klasycznych.

Szyfry przestawieniowe:

- szyfry permutacyjne;
- przestawiają porządek liter;
- alfabet wejściowy = alfabet wyjściowy;
- szyfrogram ma ten sam rozkład częstotliwości co tekst jawny;

Przykład - szyfr transpozycji wierszy:
Tekst jest wpisywany wierszami do odpowiedniej liczby kolumn. Zmieniany zostaje porządek kolumn zgodnie z kluczem. Szyfrogram otrzymywany jest poprzez odczytanie go uporządkowanymi zgodnie z kluczem kolumnami

Szyfry podstawieniowe:

- szyfry monoalfabetyczne - każda litera zastąpiona zostaje różną losową literą alfabetu tajnego;
- szyfry polialfabetyczne - używają wielu alfabetów szyfrujących, w jednej rundzie użyty zostaje każdy z alfabetów
- szyfr podstawieniowy zastępuje każdy znak alfabetu jawnego A odpowiadającym mu znakiem alfabetu tajnego B;
- alfabet wejściowy =/= alfabet wyjściowy;
- podatne na kryptoanalizę.

Przykład - szyfr Cezara:
Przy szyfrowaniu tekstu jawnego każda litera zostaje zastąpiona literą przesuniętą o liczbę podaną w kluczu (oryginalnie 3)

7. Jakie szyfry klasyczne podatne są na kryptoanalizę statystyczno-lingwistyczną?

Szyfry podstawieniowe są podatne na kryptoanalizę, ponieważ litery używane są z różną częstością i możliwe jest dokonanie złamania szyfru za pomocą tzw. tabel częstotliwościowych (pojedynczych liter, par lub trójek). Polega to na obliczenia częstotliwości występowania danych liter lub kombinacji liter w szyfrogramie i następnie porównania jej z tabelami częstotliwości dla odpowiedniego alfabetu.

8. Dlaczego funkcja XOR jest często stosowana w kryptografii?

Operator bitowy XOR jest często stosowany w kryptografii, ponieważ w porównaniu do innych operatorów bitowych: AND i OR zwraca 0 lub 1 z takim samych prawdopodobieństwem - 50%. Operatory AND i OR zwracają te wartości z nierównym prawdopodobieństwem, AND - 25% dla 1 i 75% dla 0, a OR 75% dla 1 i 25% dla 0.

9. Jakie cechy posiada algorytm OTP - one time pad?

- Klucz:
    - użyty do szyfrowania wiadomości musi być, co najmniej tak długi jak wiadomość
    - każdy może być użyty tylko raz
    - musi być generowany w sposób całkowicie losowy
- Jeśli zastosujemy powyższe zasady, to jest udowodnione matematycznie, że metoda OTP zapewnia całkowite bezpieczeństwo (nie ma żadnych powtórzeń)
- Największą wadą tego rozwiązania jest konieczność wygenerowania i przekazania bezpiecznie bardzo długiego klucza.

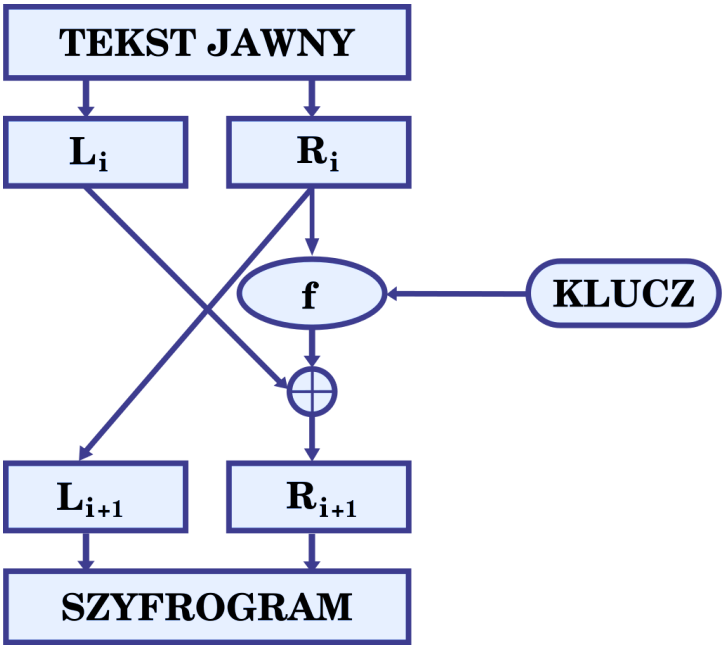
10. Przedstaw koncepcję szyfrów Shannona.

- Koncepcja szyfrów Shannona łączy szyfrowanie podstawieniowe i przestawieniowe za pomocą sieci podstawieniowo-przestawieniowych (S-P).
- Sieci S-P bazują na dwóch poznanych podstawowych operacjach szyfrujących: podstawieniach (S-bloki) i przestawieniach (P-bloki).
- Wprowadza konfuzję i dyfuzję wiadomości. Konfuzja - komplikacja, maksymalne zatarcie związku pomiędzy szyfrogramem i kluczem, dyfuzja - rozproszenie struktur statystycznych tekstu jawnego.
- “Lepiej składanie proste algorytmy, które realizują mieszanie i rozpraszanie niż poszukiwać algorytmów złożonych”

11. Co to jest struktura Feistela - scharakteryzuj i przedstaw zalety takiego przekształcenia.

Struktura Feistela - zaimplementowana koncepcja Shannona, generuje ona z tekstu jawnego szyfrogram, a z szyfrogramu tekst jawny. Struktura Feistela polega na dzieleniu tekstu jawnego na dwa bloki, całkowite szyfrowanie podzielone jest na rundy. Założenia:

- rozmiar bloku - im większy tym większe bezpieczeństwo szyfrowania;
- rozmiar klucza - większy rozmiar utrudnia zastosowanie wyczerpującego przeszukania kluczy;
- liczba rund - zwiększa bezpieczeństwo
- podklucze - większa złożoność generacji zwiększa bezpieczeństwo.



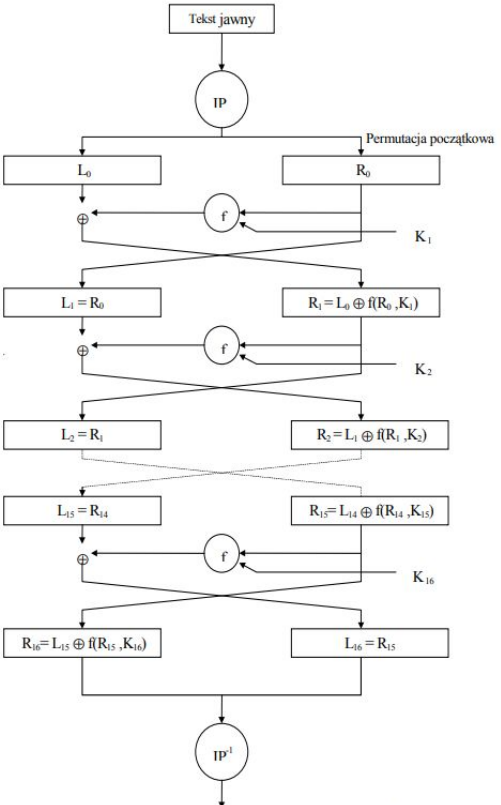
12. Jakie wymagania stawiane są współczesnym algorytmom szyfrującym?

- Jawna, łatwo dostępna i przejrzysta struktura
- Kompletnie określony i łatwy do zrozumienia
- Bezpieczny (wysoki poziom bezpieczeństwa, który wskazuje złożoność obliczeniowa)
- Możliwy do zaimplementowania sprzętowo
- Wymagający mało pamięci
- Algorytm szyfrujący musi być jednoznaczny (brak kolizji)
- Sprawdzalny (umożliwia sprawdzenie zgodności)
- Dostępny bez licencji, bezpłatny
- Skalowalny - łatwe zwiększenie lub zmniejszenie długości klucza
- Efektywny w użyciu (szybki i ekonomiczny)

13. Scharakteryzuj algorytm DES (szczegółowo).

Algorytm DES (Data Encryption Standard):

- działanie swoje opiera na strukturze Feistela;
- szyfruje wiadomości 64 bitowe używając 56-bitowego klucza;
- na starcie dokonywana jest permutacja początkowa bloku;
- blok wejściowy dzielony jest na dwie równe części: lewą i prawą;
- następnie wykonywanych jest 16 rund jednakowych operacji, nazwanych funkcjami f;
- po 16 rundach lewa i prawa strona są łączone i poddawane permutacji końcowej.

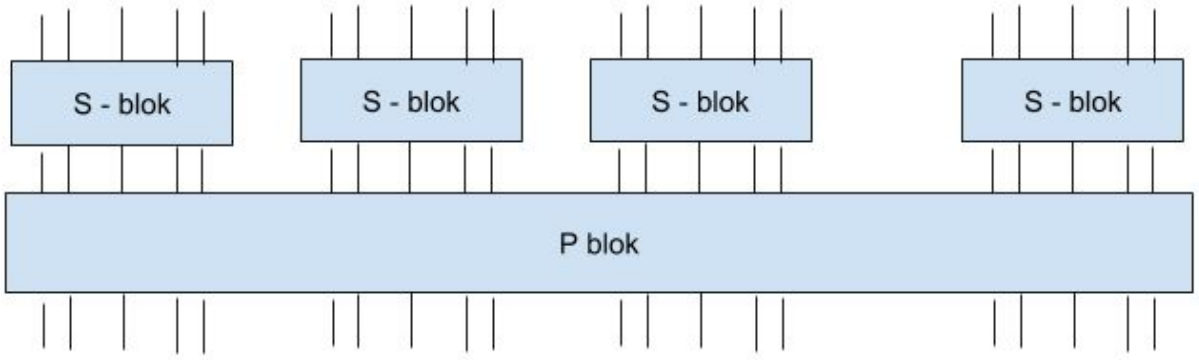


14. Wyjaśnij rolę i budowę s-bloków w algorytmie szyfrującym.

S-blok to blok podstawień, każdy bit wyjścia zależy od każdego bitu wejścia. Powoduje konfuzję bitów (zatarcie zależności pomiędzy szyfrogramem a kluczem). Nieliniowe podstawienie, 6 bitów na wejściu, 4 bity na wyjściu, 4 funkcje 6. argumentowe.

15. Wyjaśnij rolę i budowę p-bloków w algorytmie szyfrującym.

Są to bloki przestawieniowe, powinny być szybkie i zajmować mało pamięci, ich zadaniem jest powodowanie dyfuzji bitów, czyli rozproszenia struktur statystycznych tekstu jawnego.



16. Jakie cechy powinien posiadać blok S-P

Połączenie 14 i 15.

17. Scharakteryzuj ogólnie algorytm AES (ogólnie!).

AES (Advanced Encryption Standard):

- Długość przetwarzanego bloku: 128 bitów;
- Długość klucza: 128, 192, 256 bitów;
- Podczas jednej rundy algorytmu dokonywane są 4 różne operacje:
    - Podstawienia ByteSub() - nieliniowa zamiana, podczas której każdy bajt zamieniany jest innym;
    - Przesunięcia ShiftRows() wierszy w tablicy stanów - etap transpozycji, podczas którego trzy ostatnie wiersze macierzy stanu są cyklicznie zmieniane określoną ilośc razy;
    - Mieszanie MixColmns() danych z każdą kolumną tablicy stanów;
    - Dodawania AddRoundKey() klucza rundowego do tablicy stanu.

18. Tryby pracy szyfrów blokowych, po co je stosujemy, charakterystyczne zastosowania.

- ECB (Electronic Code Book):

    - Najprostszy sposób szyfrowania, każdy z bloków wiadomości jest szyfrowany i deszyfrowany oddzielnie;
    - Umożliwia przeprowadzanie (de)szyfrowania przy pomocy wielu wątków równocześnie
    - Nie występuje zaciemnianie otrzymywanego szyfrogramu
- CBC (Cipher Block Chaining):
    - wykorzystuje wektor inicjujący IV, który w celu utrzymania bezpieczeństwa powinien zostać wybrany w sposób losowy;
    - polega na dodawaniu operacji XOR każdego kolejnego bloku tekstu jawnego do poprzednio otrzymanego bloku szyfrowany. Dopiero wynik tego działania jest poddawany szyfrowaniu;
    - pierwszy blok jest poddawany operacji XOR razem z wektorem inicjującym;
    - zakłamanie jednego bitu tekstu jawnego powoduje całkowite uszkodzenie szyfrogramu natomiast zakłamanie jednego bitu szyfrogramu powoduje uszkodzenie dwóch odszyfrowanych bloków;
    - szyfrowanie w trybie cbc może być przeprowadzone tylko na jednym wątku, ale proces deszyfrowania może odbywać się z wykorzystaniem wielu wątków.
- CFB (Cipher Feedback):
    - podobna struktura do CBC, również wykorzystuje IV;
    - szyfrowane nie są bloku tekstu jawnego, lecz wymieszane dane z poprzedniej rundy, do których dodaje się oryginalne bity wiadomości;
    - w kroku pierwszym szyfrowany zostaje IV a następnie zostaje on dodany XOR do pierwszego bloku tekstu jawnego;
    - zakłamanie 1 bitu tekstu jawnego uszkadza aktualny blok szyfrogramu i wszystkie następne, a zakłamanie 1 bitu szyfrogramu uszkadza 2 bloki tekstu;
    - szyfrowanie - 1 wątek, deszyfrowanie - wiele wątków;
    - tekst jawny nie musi być wielokrotnością rozmiaru jednego bloku.
- OFB (Output Feedback):
    - szyfrowanie w trybie OFB upodabnia się do szyfrowania strumieniowego, ponieważ wytwarza ono strumień bitów klucza który, który następnie jest łączony z pojedynczym blokiem tekstu jawnego za pomocą operacji XOR;
    - początkowo szyfrowany jest IV, następnie poddawany szyfrowaniu jest wynik szyfrowania z poprzedniego kroku;
    - szyfrowanie i deszyfrowanie może odbywać się tylko na 1 wątku;
    - uszkodzenie jednego bitu tekstu jawnego bądź szyfrogramu powoduje zakłamanie jednego, odpowiadającego mu, bitu odpowiednio szyfrogramu lub tekstu jawnego.

19. Jak działają samosynchronizujące się szyfry strumieniowe?

- Występuje sprzężenie, klucz jest zależny od jakiegoś stałego n w tekście jawnym. Zmiana tekstu zmieni klucz szyfrujący.
- Są bardziej odporne dlatego, że cechy statystyczne związane z tekstem jawnym są rozproszone.
- Wadą jest to, że jeżeli pojawi się błąd będzie on propagowany dalej

20. Scharakteryzuj generator BBS.

- Generator BBS (Blum Blum Shub) - generator liczb pseudolosowych;
- Algorytm oparty jest na obliczaniu reszt kwadratowych modulo *n*;
- Generator BBS jest dość powolny, ale za to bezpieczny. Przy odpowiednich założeniach, odróżnienie jego wyników od szumu jest równie trudne jak faktoryzacja n.
- Lista kroków:
    - Bierzemy dwie duże liczby pierwsze *p* i *q*, które są kongruentne z 3 modulo 4.
    - Iloczyn *p*q=n* nazywamy liczbą Bluma.
    - Następnie wyznaczamy inną losową liczbę całkowitą *x* (ziarno), która jest względnie pierwsza z *n*, czyli NWD(x, n)=1 i obliczamy x_0 z wzoru $x_0=x^2 \ mod \ n$.
    - W kolejnych krokach oblicza się następne wartości x_i z wzoru $x_i=x_{i-1}^2 \ mod \ n$.
    - Wynikiem każdego kroku jest 1 lub 0 w zależności od parzystości x_i.

21. Scharakteryzuj generator RSA.

- RSA - asymetryczny algorytm kryptograficzny, może być stosowany do szyfrowania jak i do podpisów cyfrowych. Generuje on pary kluczy (prywatnego i publicznego).
- Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych.
- Lista kroków:
    - Wybieramy dwie liczby pierwsze *p* i *q*.
    - Obliczamy *n=p*q*.
    - Obliczamy *phi=(p-1)(q-1).*
    - Generujemy *e* jako liczbę względnie pierwszą z *phi* czyli taką, która jest liczbą pierwszą i dla której największy wspólny dzielnik z *phi* wynosi 1.
    - Generujemy *d* w taki sposób, aby spełniona była zależność: iloczyn *e* i *d* przystaje do 1 modulo *phi*. Co oznacza, że *phi* dzieli wyrażenia $e \cdot d - 1$.
    - Para *e* i *n* stanowią klucz publiczny, natomiast *d* i *n* klucz prywatny.

22. Jakie cechy powinien posiadać dobry generator ciągów losowych?

- Powinien spełniać testy:
    - Zer i jedynek - test zliczający wystąpienia zer i jedynek;
    - Serii i długiej serii - testy skupiające się na szukaniu i kontrolowaniu maksymalnego podciągu następujących po sobie zer lub jedynek;
    - Pokerowy - test dzielący ciąg bitów na segmenty 4-bitowe i kontrolujący liczbę wystąpień każdej możliwej 4 (16 możliwych).
- Znając dowolnie długi ciąg nie jesteśmy w stanie przewidzieć jaki będzie kolejny element.
- Zwiększając ciąg o jeden bit, zmieniamy wielomian, który generuje ten losowy ciąg.

23. Własności dobrej funkcji skrótu.

- Bezkolizyjność:
    - Słaba - mając wejście, które daje jakieś wyjście. nie możemy dobrać do tego wejścia innego wejścia, które dałoby nam kolizję;
    - Odporność na kolizje - dla dowolnych losowych wejść, nie uzyskamy kolizji.
- Jednokierunkowość:
    - Obliczenie skrótu powinno być wielomianowe;
    - Odwrotnie powinna być złożoność wykładnicza.
- Własność kompresji danych - kompresujemy dowolny ciąg do skrótu o danej długości
- Złożoność obliczeniowa - mając dane łatwo obliczyć skrót

24. Opisz proces przekształcenia wiadomości m (dowolnej długości) w skrót.

Mając wiadomość M o długości 1MB i do dyspozycji funkcję skrótu h, to aby obliczyć skrót:

- dzielimy wiadomość na bloki;
- jeśli blok jest niepełny (tzn. fragment danych nie jest równy wielkości bloku, czyli rozmiar danych wejściowych nie był wielokrotnością rozmiaru bloku), należy go sztucznie uzupełnić, np. poprzez dodanie samych 1 lub 0, skopiowanie fragmentu danych z początku, dodanie na końcu rozmiaru wiadomości;
- Każdy blok trafia do funkcji. Wartość następnego bloku jest obliczana na podstawie poprzedniego;

25. Czym różni się MDC od MAC?

MDC*(Manipulation Detection Code)*	**MAC***(Message Authentication Code)*
brak klucza	klucz
sprawdza integralność	służy do uwierzytelniania

26. Jakie wyróżniamy różne klasy funkcji skrótu ze względu na ich budowę?

- Z wykorzystaniem szyfrów blokowych:
    - z kluczem lub bez klucza;
    - służące do uwierzytelniania lub nie;
    - bezpieczne.
- Dedykowane, stworzone wyłącznie do wyznaczania skrótu:
    - wszystkie z rodziny MD i SHA;
    - bardzo szybkie.
- Asymetryczne - w konstrukcji korzystają z arytmetyki modularnej:
    - najwolniejsze i rzadko stosowane;
    - np. za pomocą BBS stworzyć funkcję skrótu.

27. Omów zastosowania funkcji skrótu.

- Usługi certyfikacyjne, podpis cyfrowy - nierozerwalnie związane z funkcjami skrótu;
- Sprawdzanie integralności danych: przesłanych, plików w systemie operacyjnym, danych w bazie danych;
- Uwierzytelnianie - obliczanie skrótu hasła klienta, który staje się tajnym kluczem;
- Protokół wymiany klucza w IPSec używa funkcji skrótu do generacji ciągów pseudolosowych;
- Bezpieczna komunikacja - weryfikacja integralności, uwierzytelnienie wiadomości.

28. Ataki na funkcje skrótu:

29. Jak znajdujemy liczby pierwsze?

- Przeszukiwanie (mało efektywne)
- Sito Eratostenesa - algorytm znajdowania liczb pierwszych z zadanego przedziału
- Test Fermata - probabilistyczny test umożliwiający sprawdzenie czy dana liczba jest złożona, czy pierwsza
- Spirala Ulama - graficzna metoda pokazywania pewnych niewyjaśnionych do dziś prawidłowości w rozkładzie liczb pierwszych,

30. Co to są liczby Carmichaela

Liczby Carmichaela to w teorii liczb takie liczby złożone, dla których teza Małego Twierdzenia Fermata jest prawdziwa. Czyli liczba naturalna n jest liczbą Carmichaela, gdy:

- jest liczbą złożoną,
- dla każdej liczby naturalnej a z przedziału 1<a<n, względnie pierwszej z *n*, liczba $(a^{n-1}-1)$ jest podzielna przez *n*.

31. Co to są liczby Mersenne'a?

Są to liczby postaci $M_n=2^n-1$, gdzie *n* jest liczbą naturalną. Wiadomo, że jeżeli n jest liczbą złożoną, to liczba M_n jest także liczbą złożoną. Prawdziwe jest twierdzenie, że jeżeli M_n jest liczbą pierwszą to *n* musi być liczbą pierwszą, ale niekoniecznie na odwrót. Wykaz przykładowych liczb pierwszych Mersenne'a: 2^2-1, 2^5-1, $2^{13}-1$.

32. Przedstaw algorytm Diffiego-Hellmana (szczegółowo).

Algorytm Diffiego-Hellmana oparty jest na trudności obliczania logarytmów dyskretnych w ciałach skończonych. Wykorzystywany jest do dystrybucji kluczy (nie do szyfrowania i deszyfrowania). Algorytm:

- A i B uzgadniają ze sobą w sposób jawny wybór dwóch dużych liczb całkowitych n - duża liczba pierwsza i g - pierwiastek pierwotny modulo n i gdzie 1<g<n.
- A wybiera losową dużą liczbę całkowitą x (tajną) - to będzie jej klucz prywatny i oblicza $X=g^x \bmod n$

- B wybiera losową dużą liczbę całkowitą y (tajną) - to będzie jej klucz prywatny i oblicza $Y=g^y \bmod n$
- A i B przesyłają do siebie nawzajem obliczone X i Y.
- A oblicza $k=Y^x \bmod n$
- B oblicza $k=X^y \bmod n$
- k zostaje kluczem sesji.

33. Jak generujemy klucze w RSA?

Lista kroków:

- Wybieramy dwie liczby pierwsze *p* i *q*.
- Obliczamy *n=p*q*.
- Obliczamy *phi=(p-1)(q-1).*
- Generujemy *e* jako liczbę względnie pierwszą z *phi* czyli taką, która jest liczbą pierwszą i dla której największy wspólny dzielnik z *phi* wynosi 1.
- Generujemy *d* w taki sposób, aby spełniona była zależność: iloczyn *e* i *d* przystaje do 1 modulo *phi*. Co oznacza, że *phi* dzieli wyrażenia $e \cdot d - 1$.
- Para *e* i *n* stanowią klucz publiczny, natomiast *d* i *n* klucz prywatny.

34. Zastosowanie kluczy z algorytmu RSA?

Klucz publiczny:

- szyfrowanie;
- weryfikacja podpisu.

Klucz prywatny:

- deszyfrowanie;
- podpis elektroniczny.

35. Jaka jest różnica pomiędzy algorytmem RSA i Diffiego-Hellmana

Algorytm RSA	Algorytm Diffiego-Hellmana
Wykorzystywany przy szyfrowaniu/deszyfrowaniu oraz w podpisie cyfrowym	Wykorzystywany do generowania klucza sesyjnego
Bezpieczeństwo oparte na trudności faktoryzacji dużych liczb złożonych	Bezpieczeństwo oparte na trudności obliczania logarytmów dyskretnych w ciałach skończonych.

36. Jakie znasz inne algorytmy szyfrowania asymetrycznego oprócz RSA i D-H?

- El Gamala
- Rabina
- Algorytm Plecakowy
- DSA

37. Jakie cechy powinien posiadać podpis elektroniczny?

- poufność;
- integralność;
- niezaprzeczalność nadania i odbioru - by nie można było wyprzeć wysłania, odebrania. Nie zawsze jest to wymagane, ale czasami jest to konieczne;
- znacznik czasu - jest opcjonalny, przeciwdziała atakom.

38. Etapy tworzenia i weryfikacji podpisu elektronicznego.

Podpis cyfrowy jest unikatową wartością dołączaną do pliku przez specjalne oprogramowanie.
Etapy tworzenia podpisu:

- Tworzenie skrótu wiadomości;
- Szyfrowanie skrótu kluczem prywatnym;
- Przesłanie podpisanego skrótu wraz z wiadomością do adresata.

Weryfikacja podpisu:

- odszyfrowanie skrótu za pomocą klucza publicznego
- obliczenie skrótu dla przesłanej wiadomości;
- porównanie skrótów.

39. Co to są ślepe podpisy cyfrowe?

- Forma podpisu cyfrowego, w której podpisywany dokument nie jest znany osobie podpisującej
- Poświadcza się autentyczność posiadania wiadomości przez właściciela w danym czasie (przydatne np. przy rozstrzyganiu roszczeń dot. wniosków patentowych czy umów); podpis taki może potem być zweryfikowany z wiadomością
- Wykorzystywane na ogół w protokołach opartych na prywatności, w których autor wiadomości i podpisujący to różne osoby
- Zaślepianie wiadomości: $(m*k^e)^d$

40. Z jakich pól składa się certyfikat cyfrowy?

- wersja
- numer seryjny
- wydawca certyfikatu
- ważność
- podmiot dla którego certyfikat został wystawiony
- klucz publiczny oraz podpis organu wydającego certyfikat

41. Na czym polega weryfikacja certyfikatu?

Weryfikacja certyfikatu polega na prześledzeniu łańcucha zaufania zakończonego przez organ nadrzędny, cieszący się powszechnym zaufaniem , który sam dla siebie wystawia certyfikat.

42. Funkcje PKI

- Rejestracja (*Registration*)
- Certyfikacja (*Certification*)
- Generacja kluczy (*Key generation*)
- Odnawianie kluczy (*Key update*)
- Certyfikacja wzajemna (*Cross-certification*)
- Odwołanie certyfikatu (*Revocation*)
- Odzyskiwanie klucza (*Key recovery*)

43. Co to jest i jaka jest struktura CRL?

- Lista unieważnionych certyfikatów (lista CRL, ang. Certificate Revocation List) – lista certyfikatów unieważnionych przez organ certyfikujący z różnych powodów.
- Wyróżnia się dwa różne stany cofnięcia certyfikatu:
  - Wstrzymany – certyfikat może zostać przywrócony (jeżeli np. użytkownik stracił swój klucz prywatny, odzyskał go i ma pewność, że nikt postronny nie miał do niego dostępu, to może ponownie przywrócić ważność certyfikatu).
  - Unieważniony – świadectwo jest nieodwracalnie cofnięte.
- CRL zadba o obsługę certyfikatów które stają się nieważne przed datą wygaśnięcia. Może się tak stać np. przy ujawnieniu klucza prywatnego.

44. Jakie mogą być powody odwołania certyfikatów?

- kompromitacja kluczy
- kompromitacja klucza organu wydającego certyfikaty CA
- zmiana danych subskrybenta
- zastąpienie (odnowienie) klucza
- zaprzestanie operacji z wykonywaniem klucza
- zawieszenie (wstrzymanie) certyfikatu
- zamknięcie firmy

45. Jaka jest różnica pomiędzy protokołem LDAP i OCSP?

LDAP (*Lightweight Directory Access Protocol*) - protokół, który daje wgląd do bazy danych certyfikatów, umożliwia: czytanie z repozytorium, przeszukiwanie repozytorium i modyfikację. Dzięki LDAP:

- otrzymujemy więcej informacji niż tylko czy certyfikat jest ważny;
- otrzymujemy informacje o tym kiedy będzie następna aktualizacja bazy;
- informacja o certyfikatach z bazy danych może być długa i sprawiać problemy z wydajnością

OCSP (*Online Certificate Status Protocol*) - protokół komunikacyjnym pomięzdy systemem informatycznym odbiorcy usług certyfikacyjnych a serwerem usługowym. Protokół OCSP działa następująco:

- aplikacja wysyła zapytanie o ważność certyfikatu do serwer OCSP;

- serwer odpowiada na zapytanie: poprawny (wg aktualnej wiedzy serwera certyfikat nie jest unieważniony w chwili zapytania), unieważniony (wstrzymanie lub unieważnienie certyfikatu), nieznany (serwer nie posiada informacji nt certyfikatu).

46. Jaka jest różnica pomiędzy uwierzytelnianiem a autoryzacją?

Uwierzytelnianie - jednoznaczna weryfikacja tożsamości danego użytkownika np. za pomocą hasła, bądź bardziej zaawansowanych metod takich jak dowód z wiedzą zerową.
Autoryzacja - polega na sprawdzeniu, czy dana operacja dla danego użytkownika jest dozwolona (musimy mieć prawo dostępu). Autoryzacja ma miejsce po pomyślnym uwierzytelnieniu.

47. Jakie znasz protokoły uwierzytelniania?

PAP (*Password Authentication Protocol*):
- najniższy poziom bezpieczeństwa, używa haseł w postaci zwykłego tekstu;
- używany, gdy nie ma możliwości bezpieczniejszej formy weryfikacji.

CHAP (*Challenge Handshake Protocol*):
- udoskonalenie PAP, wyższy poziom bezpieczeństwa;
- zapewnia węzłom zgłaszanie tożsamości za pomocą trójfazowego uzgadniania;
- zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji, wykorzystuje MD5.

EAP (*Extensible Authentication Protocol*):
- urządzenie uwierzytelniające wysyła do użytkownika zapytania w celu uwierzytelnienia go;
- w wysłanym pakiecie znajduje się pole, wskazujące rodzaj zapytania, np. żądanie hasła czy skrótu SHA-2;
- najwyższy poziom bezpieczeństwa ze względu na elastyczność sposobu uwierzytelniania.

48. Jakie wymogi muszą obowiązywać algorytmy podziału sekretu (t,n)
- Poprawności - conajmniej t spośród n udziałów pozwala na odtworzenie sekretu s
- Prywatności - znajomość mniejszej niż t liczby kanałów sekretu nie umożliwia odczytania sekretu

49. Omów metodę trywialną podziału sekretu.

Metoda trywialna podziału sekretu oznacza, że wszystkie wygenerowane udziały są konieczne do odtworzenia sekretu.
Sekret reprezentowany jest za pomocą liczby całkowitej *s* z zakresu (*0, k-1*). Fragmenty sekretu $s_1, s_2, \ldots, s_{n-1}$ są generowane losowo, i każdy z fragmentów jest mniejszy od k.
Ostatni udział generowany jest za pomocą wzoru:

$$s_n = (s - s_1 - s_2 - \ldots - s_{n-1}) \bmod k$$

Odtworzenie sekretu jest realizowane za pomocą wzoru:

$$s = (s_1 + s_2 + \ldots + s_n) \bmod k$$

50. Co to jest kryptografia wizualna?

- Metoda podziału sekretu na udziały, później złożenie tych udziałów może się odbywać bez sprzętu komputerowego;
- Matematycznie kryptografia wizualna jest bardzo bezpieczna. Jeżeli nie wiemy co jest sekretem to nie dojdziemy co zostało zaszyfrowane;
- Zalety:
    - łatwa implementacja;
    - nie potrzeba programu deszyfrującego;
    - udział może być wysłany mailem;
- Wady:
    - odszyfrowany sekret posiada zakłócenia;
    - dopasowanie folii podczas odszyfrowywania musi być bardzo dokładne
    - rozmiar odszyfrowanego sekretu jest różny od oryginału

51. Omów algorytm steganografii - najmniej znaczącego bitu

- Algorytm najmniej znaczącego bitu, *LSB*, modyfikuje ostatnie bity poszczególnych kanałów jednego piksela obrazu, w taki sposób, aby zmiana została możliwie niewidoczna, a żeby móc zapisać na nich zaszyfrowaną wiadomość.
- Wynik zależy ściśle od liczby bitów przeznaczonych do zapisu pojedynczego piksela: im więcej bitów opisuje dany piksel tym mniejsze znaczenia ma dla całkowitego odczucia odbiorcy modyfikacja jednego lub kilku ostatnich bitów.
- Oznaczony w taki sposób można łatwo sfałszować, dokonując np:
    - zamiany formatu;
    - zmniejszając głębię koloru;
    - poddając go kompresji;

52. Omów algorytm steganograficzny - patchwork.

- polega na osadzaniu w chronionym obrazie informacji pseudolosowej;
- wymaga stosowania generatora liczb pseudolosowych uruchamianego za pomocą tajnego klucza;
- wygenerowane ciągi pseudolosowe oznaczają obszary w obrazie, których jasność została nieznacznie zmieniona w taki sposób, aby nie dało się tego zauważyć;
- wyciąganie znaku wodnego z obrazu opiera się na zainicjalizowaniu w ten sam sposób tego samego generatora liczb pseudolosowych i odtworzeniu obszarów przywracając im pierwotną wartość oraz sprawdzają zapamiętaną sumę różnic obszarów w celu sprawdzenia integralności.

53. Omów z jakich protokołów składa się protokół SSL

SSL dzieli się na dwa podprotokoły (warstwy funkcjonalne):

- warstwa komunikatów - używa warstwy rekordów do przesyłania danych pomiędzy serwerem a klientem, gdy tworzą ze sobą połączenie (faza negocjacji);
- warstwa rekordów - przesyłanie bezpiecznym połączenie rekordów (bloki danych).

SSL zapewnia:

- szyfrowanie danych;
- uwierzytelnienie 1. lub 2. stronne;
- integralność wiadomości;

54. Omów sesję protokołu SSH.

Opiera się na RSA

- uwierzytelnianie serwera wobec klienta;
- ustanawianie bezpiecznego połączenia między serwerem i klientem;
- uwierzytelnianie klienta wobec serwera;
- logowanie klienta w systemie operacyjnym serwera;
- praca użytkownika na zdalnych serwerach.

55. Omów PGP.

- *Pretty Good Privacy* - jeden z protokołów poczty elektronicznej;
- Wykorzystuje 4 mechanizmy przetwarzania danych:
    - szyfrowanie
    - podpis cyfrowy
    - kompresja
    - kodowanie
- generowanie komunikatu PGP
    - sygnowanie komunikatu:
        - PGP odszukuje swój klucz prywatny o podanym ID w bazie kluczy prywatnych
        - PGP prosi o podanie hasła w celu uzyskanie niezaszyfrowanego klucza prywatnego, skrót hasła służy do odszyfrowania klucza prywatnego
    - szyfrowanie komunikatu:
        - PGP generuje klucz sesji i szyfruje komunikat algorytmem symetrycznym z użyciem klucza sesji
        - PGP szyfruje klucz sesji za pomocą klucza jawnego odbiorcy z bazy kluczy jawnych
- zarządzanie kluczami jawnymi - sieć zaufania
    - w bazie kluczy jawnych w polu zaufania wpisywane jest zaufanie użytkownika do właściciela danego klucza
    - można ufać całkowicie lub częściowo
    - wszystkie klucze, których właścicielom ufamy są sygnowane przez nas
    - dwie częściowo zaufane sygnatury poświadczają klucz

56. Rodzaje wirusów komputerowych.

- worms - robaki, szybko się rozmnażają w systemie, celem jest przeniesienia z jednego do drugiego komputera przez internet, spowalniają system;
- bootkit - uruchamia się podczas bootowania systemu ukrywając swoją obecność przed programami antywirusowymi;
- rootkit - uruchamia się jako administrator systemu ze wszelkimi uprawnieniami
- koń trojański - nie propaguje się, zaciemnia swoje intencje;
- sniffer - śledzi ruch sieciowy;
- adware - wyświetla reklamy;
- spyware - śledzi zachowania użytkownika;
- ransomware - wyłudza okup;
- coinminer - kopie kryptowaluty.

57. Jakie znasz metody klasyfikacji systemów IDS/IPS?

- według źródeł informacji:
    - sieciowe;
    - węzłowe;
    - hybrydowe;
- według metod analizy:
    - analiza sygnatur;
    - analiza anomalii;
- według typów odpowiedzi
    - aktywne;
    - pasywne;

58. Różnica pomiędzy systemami IDS sieciowymi, a węzłowymi:

Systemy IDS sieciowe	**Systemy IDS węzłowe**
skanują całą sieć i wykrywają podejrzane zachowania lub ataki w sieci	skanują tylko ruch skierowany do jednego hosta
wykrywa ataki z sieci zewnętrznej	wykrywa ataki pochodzących z tej samej sieci
składają się z wielu rozproszonych agentów	system ograniczony do jednego hosta w sieci
ma możliwość wykrywania ataków DoS/DDos	

59. Co jest bardziej skuteczne wykrywanie ataków oparte na sygnaturach czy na detekcji anomalii

Wykrywanie oparte na sygnaturach	**Wykrywanie oparte na detekcji anomalii**
poszukuje wykrytych wcześniej szablonów zachowań i wykonanych instrukcji	uczy się modelu zachowań poprawnych i porównuje nowe (aktualne) zachowania z tym modelem
nowe ataki nie zostaną wykryte, bo nie ma dla nich sygnatury	pozwala wykryć ataki bez specjalistycznej wiedzy o nich
szybkie i trafne wykrycie zastosowanej metody lub narzędzia ataku, umożliwia szybką reakcję	detektory anomalii mogą generować dane wykorzystywane później w celu definiowania sygnatur dla detektorów nadużyć
musimy dbać o aktualizowanie bazy sygnatur	wymaga rozległych “zbiorów treningowych” wydarzeń systemowych w celu zdefiniowania “normalnego” zachowania systemu
nie powoduje dużej liczby fałszywych alarmów	sygnalizuje dużą liczbę fałszywych alarmów

60. Jakie mogą być odpowiedzi systemu IDS na atak?

- aktywne - zautomatyzowane działania, podejmowane gdy wykryte zostaną określone typy włamań:
    - zbieranie dodatkowych informacji (“system zaczyna “nasłuchiwać w celu znalezienia informacji, która przesądzi o dalszej akcji);
    - zmiana środowiska (zatrzymanie ataku i zablokowanie kolejnych działań ze strony atakującego - np. blokada adresu IP, ignorowanie pakietów od tego IP);
    - podjęcie akcji przeciwko intruzowi (niezalecane, ponieważ wielu atakujących używa fałszywych adresów IP, niesie to ryzyko uszkodzenia przypadkowych komputerów w sieci)
- pasywne - dostarczanie informacji operatorom systemu, zostawiając podejmowanie akcji na podstawie przekazanych informacji ludziom za to odpowiedzialnym:
    - alarmy i powiadomienia (informują operatorów o ataku najczęściej w formie powiadomienia na ekranie monitora lub na telefon komórkowy osoby odpowiedzialnej za bezpieczeństwo sieci, szczegółowość wiadomości jest różna);
    - pułapki SNMP (*Simple Network Management Protocol*) - wysyłanie alarmów do centralnej konsoli zarządzającej, gdzie mogą one być następnie obsłużone przez personel nadzorujący;
    - zalety:

- możliwość przystosowania całej infrastruktury sieciowej do odpowiedzi na wykryty atak;
- przeniesienie obciążenia systemu na system inny od atakowanego;
- możliwość użycia wspólnych kanałów komunikacyjnych.

61. Porównaj atak słownikowy z atakiem przez wyczerpujące przeszukiwanie.