1. Co to znaczy **n** szyfr Hilla

   Każdą literę koduje się jako numer. Najczęstszy schemat korzysta z układu: A=0, B=1, …, Z=25, jednak nie jest to niezmienna zasada tego szyfru. Blok **n** jest przedstawiany w postaci wektora o **n** wymiarach. Następnie jest mnożony przez macierz o wymiarach **n** × **n**, modulo 26 (wartość wynika z liczby elementów w układzie). Cała tablica traktowana jest jako klucz. Należy sprawdzić czy macierz jest odwracalna (aby upewnić się, że deszyfrowanie będzie możliwe).

2. Scharakteryzuj szyfry symetryczne

   Cechy:

   - Jeden klucz

   Szyfry podstawieniowe:

   - Monoalfebetyczne – szyfr cezara, klasyczne podstawienia, Atbash, Rot13, Nihilist
   - Polialfabetyczne – szyfr Vigener'a, Byte Addition, XOR, szyfr Vernam'a
   - Poligramowe - Hill, Playfair
   - Homofoniczne

   Szyfyr przestawieniowe

   Szyfry złożone (ADFGVX)

3. Szyfr homofoniczny – pojedynczemu zankowi tekstu jawnego przyporządkowuje się jeden z kilku przypisanych znakow.
4. Szyfr podstawieniowy

   System szyfrowania, w którym każda litera tekstu jawnego zostaje zastąpiona innym znakiem, ale zostaje na swoim miejscu

5. Szyfr przestawieniowy (permutacyjny)

   System szyfrowania, w którym każda litera tekstu jawnego zmienia swoją pozycję w tekście, ale zachowuje swoją tożsamość.

6. Scharakteryzuj szyfry asymetryczne

   Przykładowe algorytmy:

   - RSA

   Cechy:

   - Dwa klucze
   - Czasochłonne
   - Inny aparat matematyczny od symetrycznych (nie wykorzystują historycznych algorytmów)
   - Używane do podpisu elektronicznego
   - Szyfruje się kluczem publicznym.
   - Podpisuje i deszyfruje się kluczem prywatnym.
   - Używane do szyfrowania niedużych informacji, np. klucz symetrycznych

7. Co to jest entropia i od czego zależy

   Entropia jest to miara losowości. W kontekście laboratorium jest to miara losowości wystąpień znaków w tekście jawnym lub zaszyfrowanym. Zależy od prawdopodobieństwa wystąpienia każdego znaku w tekście. Jest największa gdy prawdopodobieństwo wystąpienia każdego znaku jest równe.

8. Co to są szyfry polialfabetowe i monoalfabetowe

   - Polialfabetowe: uogólnienie szyfru monoalfabetycznego na większą liczbę przekształceń. Szyfra taki składa się z n przekształceń, takich, że pierwszą literę szyfruje się pierwszym przekształceniem, drugą drugim itd. Następnie

przekształcenia są powtarzane. Współcześnie tylko znaczenie w konteksie historyczne

- Monoalfabetowe: szyfr, w którym jednej literze alfabetu tajnego odpowiada dokładnie jedna litera alfabetu jawnego. Praktycznie nie zapewnia bezpieczeństwa, bo bardzo łatwo go złamać

$$f(a) = (a + k) \bmod n$$

a – szyfrowana litera

k – klucz

n – liczba liter w alfabecie

9. Znaczenie kluczy w asymetrycznych

   Są dwa klucze:

   - Prywatny, który służy do deszyfrowania/podpisywania
   - Publiczny, który służy do szyfrowania

10. Co to szyfrowanie?

    Szyfrowanie to sposób zwiększania bezpieczeństwa wiadomości lub pliku poprzez stosowanie metod powodujących utajnienie informacji. Szyfrowania pozwala na bezpieczne przechowywanie i przesyłanie poufnych danych, ponieważ zaszyfrowany tekst jest zniekształcony, nie przypomina tekstu jawnego. Innymi słowami jest to proces, podczas którego stosowany jest algorytm, który transformuje dane do postaci niezrozumiałej. Algorytm szyfrujący przyjmuje różne parametry, między innymi klucz szyfrujący.

11. Co to klucz kryptograficzny?

    Informacja (ciąg symboli, znaków) wykorzystywana w procesie szyfrowania (lub deszyfrowania) do utajniania (lub odtwarzania) wiadomości jawnej.

12. Entropia w RSA – jaka jest maksymalna i dlaczego?

    Algorytm RSA koduje każdy znak w postaci pary dwóch 16-kowych cyfr, z których każdą można wybrać na 16 sposobów, co daje 256 możliwości reprezentacji. Każdy z bloków może przyjąć 1 z 256 wartości (para 2 szesnastkowych cyfr), dlatego alfabet składa się z 256 znaków. W przypadku, gdy prawdopodobieństwa poszczególnych zdarzeń w zbiorze są równe, czyli maksymalnej entropii, można stosować wzór w postaci uproszczonej:

    $H(x) = \log_2(n)$ n – wielkość zbioru, czyli dla n=256 entropia wynosi H=8

13. Czy wielokrotne szyfrowanie zwieksza moc szyfrow polialfabetowych

    Jeżeli nie użyje się dłuższego klucza to nie, bo w efekcie otrzymuje się po prostu szyfrogram zaszyfrowany za pomocą innego klucza, czyli nie zwiększa się moc.

14. RSA

    - Jest to algorytm szyfrowania asymetrycznego
    - Zaprojektowało go 3 ziomków
    - Jest to algorytm, który można użyć zarówno do szyfrowania jak i do podpisów elektronicznych (cyfrowych)
    - Wykorzystuje operacje mnożenia i faktoryzacji
    - Wykorzystuje dwa klucze – publiczny i prywatny; Klucz publiczny może być udostępniany i jest używany do zaszyfrowania danych, a klucz prywatny służy do ich rozszyfrowania i jest tajny (służy również do podpisu)
    - Klucze generowane są z wykorzystaniem dużych liczb pierwszych i funkcji Eulera
    - Wadą jest długi czas deszyfrowania

15. Kiedy entropia jest maksymalna?

Entropia jest maksymalna, kiedy prawdopodobieństwa, wystąpień poszczególnych znaków, są równe. Jest wtedy największe rozproszenie danych, nic nie występuje częściej od reszty.

16. Z czego wynika siła współczesnych algorytmów blokowych
17. Z czego wynika siła algorytmów asymetrycznych

Z trudności rozkładu dużych liczb złożonych na czynniki pierwsze.

18. Z czego wynika siła algorytmów symetrycznych blokowych

19. Jakie są działania przy algorytmach symetrycznych blokowych
    - Permutacje znaków/bitów
    - Permutacje bloków
    - Podstawienia
    - Podstawienia nieliniowe
    - Kompresje
    - Rozciąganie

20. W których algorytmach po ponownym zaszyfrowaniu możemy otrzymać tekst jawny
    - Cezara
    - Rot 13

21. Co to klucz kryptograficzny i jakie wymagania przed nim stawiamy

Informacja (ciąg znaków) wykorzystywana w procesie szyfrowania (lub deszyfrowania) do utajniania (lub odtwarzania) wiadomości jawnej.

Wymagania:

- Klucz musi być ukryty, nie można go ujawniać, ponieważ nawet część ujawnionego klucza sprawia, że o wiele łatwiej jest odszyfrować szyfrogram.
- Im dłuższy klucz tym trudniej jest go złamać (metoda brute force). Zakładając, że **k** to długość klucza, a **T** to czas wykonywania pojedynczej operacji to maksymalny czas łamania szyfru można określić

  wzorem: **2^k * T**, gdzie większość kluczy zostaje znalezionych w połowie czasu więc w często czas łamania szyfru wynosi: **2^(k-1) * T**

22. Od czego zależy liczba kluczy w alg złożonych?

    Szyfry złożone to szyfry wykorzystujące jednocześnie podstawienie i przestawienie (permutacje) w tzw. Rundach. W każdej rundzie dokonuje się szyfrowanie podstawieniowe jednej połówki bloku wejściowego, a następnie permutację zmieniające obie połówki. W każdej rundzie przekształcenie odbywa się w oparciu o inny klucz.

    - Od długości alfabetu
    - Od rozby alfabetu ???
    - Od rodzaju algorytmu szyfrowania
    - Od długości klucza, ponieważ gdy klucz ma 1 bit to dostępne są 2 klucze, jak 2 bity to 4 klucze itd.
    - **2^n**, gdzie **n** to liczba bitów

23. Moc algorytmów złożonych

    Moc algorytmu złożonego jest równa iloczynowi mocy algorytmów składających się na niego.

24. Jak prównujemy algorytmy kryptujące

    Na podstawie:

    - Mocy
    - Długości klucza
    - Czasu
    - Zastosowania
    - Odporności na błędy

25. Co to są szyfry monogramowe i poligramowe

- Monogramowe – każdy znak tekstu jawnego jest szyfrowany osobno, np. **Cesar, Vigenere, Vernam**
- Poligramowe – tekst jawny dzielony jest na grupy, np. dwuznakowe, trzyznakowe i każda grupa jest poddawana algorytmowi szyfroania: **Playfair, Hill**

26. Propagacja błędów w szyfrach (trybach) blokowych

- ECB (Electronic codebook) – uszkodzenie jednego fragmentu bloku tekstu jawnego lub szyfrogramu powoduje uszkodzenie odpowiadającego mu fragmentu bloku szyfrogramu lub tekstu jawnego. Uszkodzenie nie wpływa na pozostałe bloki
- CBC (Cipher-block-chaining) – Uszkodzenie jednego bloku szyfrogramu powoduje jedynie uszkodzenie dwóch kolejnych bloków tekstu jawnego. Zmiana jednego bloku tekstu jawnego powoduje uszkodzenie wszystkich kolejnych bloków szyfrogramu.
- OFB (Output feedback) – Zmiana jednego fragmentu bloku tekstu jawnego lub uszkodzenie jednego bloku szyfrogramu powoduje uszkodzenie/zmianę odpowiadającego mu fragemntu bloku szyfrogramu/tekstu jawnego. Uszkodzenie nie wpływa na pozostałe bloki
- CFB (Cipher feedback) – Zmiana informacji wejściowej (tekstu jawnego) powoduje propagacje błędu na kolejne bloki szyfrogramu.
- CTR (Counter mode) – poszczególne bloki są przetwarzane niezależnie, nie ma łańcuchowania więc uszkodzenie jednego bloku nie powoduje uszkodzenia innych bloków

27. Jak rozwiązać problem długości ostatniego bloku w szyfrach blokowych’

W szyfrach blokowych w trybach EBC, CBC, CFB tekst jawny musi być sekwencją jednego lub więcej kompletnych bloków. W przypadku, gdy ostatni blok jest krótszy stosuje się jego dopełnienie do pełnej długości, najczęściej za pomocą ciągu bitów rozpoczynających się jedynką i zawierających resztę zer. Jako dobrą praktykę zaleca się uzupełnienie tekstu jawnego dodatkowym blokiem, gdy składa się on oryginalnie z pełnych bloków. Uzupełnienie komunikatu do równej długości nie zawsze jest dopuszczalne, np. sytuacji gdy szyfrogram jest zapisany tym samym buforze, co tekst jawny

28. Scharakteryzować blokowe, wady i zalety i zastosowania

    Jest w pdf. KTO PYTA NIE BLADZI, nie chce mi się już pisac

29. Zastosowanie trybów szyfrów blokowych

    - ECB – transmisja pojedynczych obietków, np. Kluczy publicznych
    - CBC – ogólna transmisja blokowa, uwierzytelnianie
    - CFB – ogólna transmisja strumieniowa, uwierzytelnianie
    - OFB – transmisja strumieniowe w kanałach wysokiego zakłócania
    - CTR – w przypadku zapotrzebowania na kanały wymagające dużej szybkości transmisji

30. Cos z tym, ze czemu klucz powinien być długi czy cos takiego

    - Długi klucz utrudnia złamanie metodami brute-force
    - Może powodować redukcję szybkości szyfrowania i deszyfrowania

31. Szyfrowanie

    Tworzenie kryptogramu (tekstu zaszyfrowanego/tajnego) na podstawie tekstu źródłowego (jawnego) i klucza (kluczy) kryptograficznych.

32. Deszyfrowanie

    Odtwarzanie tekstu jawnego na podstawie znajomości klucza (kluczy) kryptograficznych

33. Co to jest hasło kryptograficzne i jakie są z nim związane wymagania (że ciąg znaków używany jako informacja pomocnicza przy szyfrowaniu, powinien być długi, tajny etc)

    Ciąg znaków stosowany powszechnie jako tajny parametr w kryptografii oraz uwierzytelnianiu. hasło powinno cechować się dużą entropią (Różnorodnością znaków) oraz odpowiednią długością. Hasło powinno być tajne czyli trzymane w tajemnicy przed niepowołanymi osobami

34. Coś z metodami inicjalizacji rejestru przesuwnego przy szyfrach strumieniowych (nie mam pojęcia, ja znam tylko inicjalizację ciągiem pseudolosowym)

pojęcia, ja znam tylko inicjalizację ciągiem pseudolosowym) Wejściem do funkcji szyfrującej w trybach strumieniowych jest zawartość n bitowego rejesturu przesuwnego na początku szyfrowania wartość ta ustawiana jest zgodnie z pewnym wektorem inicjalizującym zawartość rejestru przesuwnego przesuwana jest w lewo o liczbę najbardziej znaczących bitów. Rejestr przesuwny przekształcany jest przez funcję szyfrująca a wynik przekształcenia sumowany jest z wejściowym segmentem tekstu jawnego.

35. Czym charakteryzują się algorytmy podstawieniowe, a czym permutacyjne

    - Podstawieniowe – zmieniają literę z alfabetu jawnego na odpowiadającą jej litere z alfabetu niejawnego, np. Cesar
    - Permutacyjne – zmieniają pozycję litery w tekście, np. algorytmy przestawienieowe

36. Co wiesz o algorytmach poligramowych. Podaj przykłady.

    Było wyżej, playFair i Hill

37. Co to jest autokorelacja

38. Co wiesz o szyfrowaniu symetrycznym blokowym

    Szyfry blokowe dziela tekst jawny na bloki o stalej dlugosci i wynikowy kryptogram ma taka sama dlugosc. Algorytmy blokowe mogą pracować roznych trybach. Przypominaja podstawieniowe w dużej skali. Wiekoszc symetrycznych algorytmow blokowych opiera się o strukturę Feistela.

39. Scharakteryzuj szyfry symetryczne i asymetryczne?

40. Co wiesz o DES?

    - Dane są szyfrowane w 64 bitowych blokach
    - Klucz ma dlugosc 56 bitow
    - Algorytm produktoy – stosuje transpozycje w kolejnych etapach (iteracjach)
    - Szyfrowanie polega na serii etapów przetwarzających 64 bitowe dane wejściowe na 64 bitowy wynik
    - Deszyfrujac wykonuje te same etapy i ten sam klucz, ale w odwrotnej kolejności
    - Najwazniejszym elementyem sa S-box, S-skrzynki

41. Dlaczego AES jest mocny?

Nikt nie wie

42. Co wiesz o szyfrowaniu wielokrotnym?

    bylo

43. Które szyfry nie wpływają na Entropię szyfrogramu uzasadnij?

    Te historyczne, co się podstawiają i ruszają, bo zmieniasz po prostu literki, a wartość entropii nie zmienia sie