Podpis cyfrowy – gwarantuje autentyczność, niezaprzeczalności, integralność
Podpis elektroniczny – deklaracja tożsamości autora, nie ma tutaj niezaprzeczalności, integralności.
Niezaprzeczalny podpis cyfrowy – nadawca nie może się wyprzeć wiadomości i musi zgodzić się na weryfikacje podpisu.
Niepodrabialny podpis cyfrowy – pozwala wykryć fałszerstwo, istnieje wiele kluczy prywatnych.
Podpis ślepy – podpisujący nie powinien poznać treści wiadomości, wykorzystanie czynnika zaciemniającego
Podpis symetryczny z arbitrem – niepodrabialny, autentyczny i niezaprzeczalność
PKI – do zarządzania kluczami publicznymi użytkowników oraz zapobiega fałszerstwom na podmianie klucza.
PKI niezbędne elementy – Ca, CR, posiadacze certyfikatów, klienci, repozytoria.
PKI funkcje – wystawianie certyf, weryfikacja certyf i tożsamości, potw tożsamości, znakowanie czasem, szyfrowanie i podpisywanie przekazu.
PKI cykl życia klucza – utworzenie, certyfikacja, rozprowadzenie, użytkowanie aktywne i pasywne, unieważnienie klucza.
PKI proces certyfikowania – użyt zgłasza się z kluczem publicznym do CA, do weryfikacji wykorzystywany jest klucz publiczny CA.
PKI przechowywanie certyfikatów – DNS, FTP, DAP, WWW, Bazy danych, X.500, OSCP
Standard X.509 definicja – definiuje schemat certyfikatu, unieważnień CRL i atrybutu
Standard X.509 składowe certyfikatu – Wersja, numer seryjny, sygnatura, informacja o wystawcy, rozszczerzenia, data ważności
Standard X.509 CRL – Certificate Revocation List, lista unieważnionych certyfikatów, są wyłącznie numery seryjne unieważnionych certyfikatów.
Model OSI-7 definicja –
Model OSI-7 warstwy – aplikacji, prezentacji, sesji, transportowa, sieciowa, łącza danych, fizyczna
Warstwa aplikacji – protokoły: FTP DNS POP3 HTTP ,interfejs transmisji danych przez aplikacje
Ataki pasywne – atakujący ma dostęp do danych w systemie, może je czytać ale nie modyfikuje
Ataki aktywne – atakujący pośredniczy w przetwarzaniu danych w systemie, może zmieniać dane
Techniki ataków
Sniffing – podsłuchiwanie tego co jest w sieci, a co nie jest dla nas
Spoofing – podszywanie się, naciąganie
Dos – zalewanie sieci nadmiarem danych
DDoS – zajmowanie wszystkich wolnych zasobów
Nmap – narzędzie do eksploracji sieci i audytów bezpieczeństwa.
DNS – Domain Name System, służy do zmiany nazw domenowych zrozumiałych dla użytkowników na adresy rozumiane dla urządzeń sieciowych
FTP – File transfer protocol, transfer plików
Telnet – Obsługa terminala w architekturze klient – serwer
LDAP – Lightweight Directory Access Protocol
Decompression bomb – generowanie nieskończenie dużego pliku
Fork-bomb – tworzenie wielu kopii programu w celu wypełnienia tablicy procesów
Brute force – systematyczne sprawdzenie wszystkich możliwych kombinacji haseł/kluczy
SSL/TLS – wykorzystuje algorytmy szyfrowania, służy do zabezpieczeń
Firewall definicja – system bezpieczeństwa, który służy do kontroli ruchu przychodzącego i wychodzącego
Firewall rodzaje – sprzętowy i programowy
Firewall typy – Stanowe i Bezstanowe
Firewall rozwiązania – Filtrowanie pakietów, proxy, VPN
Proxy – pośredniczą w transmisji, użytkownik do proxy, a proxy do serwera

NAT – zmienia adres źródłowy w nagłówku IP
VPN – Virtual Private Network – umożliwia transmisje danych przez sieć publiczną za pomocą bezpiecznego kanału
PGP- Pretty Good Privacy – służy do szyfrowania odszyfrowania i uwierzytelniania
IPSec definicja zastosowanie – w celu zabezpieczenia protokołu IP
IPSec protokoly – TCP UDP ICMP
IPSec tryb pracy – Transportowy, tunelowania
IPSec bazy danych – SPD SAD
NAT Traversal – umożliwia urządzeniom znajdującym się za NAT zestawienie bezpiecznego połączenia
IKE – Internet Key Exchange – służy do wymiany kluczy oraz zestawiania bezpiecznych połączeń
Kerberos – protokół uwierzytelniania i autoryzacji
Bezpieczeństwo sieci bezprzewodowych WIFI – WEP WPA WPA2 WPS
WEP – Wired Equivalent Privacy
TKIP – Temporal Key Integration Protocol
Bezpieczeństwo – ochrona przed oszustwami, fałszerstwai, szpiegostwem, niszczeniem danych.
Poufność – ochrona informacji przed nieautoryzowanym jej ujawnieniem
Integralność – ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem
Dostępność – czas bezawaryjnego działania usługi w stosunku do całości czasu, w którym usługa ta powinna być klientom świadczona.
Identyfikacja – możliwość rozróżnienia użytkowników
Uwierzytelnienie – proces weryfikacji tożsamości użytkownika, np. co użytkownik wie lub co ma
Odpowiedzialność – nadanie odpowiednich uprawnień użytkownikowi
Autoryzacja – proces przydzielania użytkownikowi praw dostępu do zasobów.
Safety – system nie stwarza zagrożenia dla podmiotów znajdujących się poza systemem
Security – odporność systemu na zagrożenia zewnętrzne takie jak utrata poufności czy integralność.
Ryzyko – Prawdopodobieństwo wystąpienia niepożądanego zdarzenia i skutku
Zagrożenie – możliwość niewłaściwego wykorzystania systemu.
Haker – łamanie zabezpieczeń programów komputerowych czy dostępu do systemów.
Cracker – Włamywanie do systemów lub siecikomputerowych
Wiarygodność systemu – pewność działania systemu, która pozwala mieć uzasadnione zaufanie do usług, które ten system dostarcza.
Podział zagrożeń – wewnętrzne/zewnętrzne, pasywne/aktywne/przypadkowe
Zasady tworzenia bezpiecznych haseł – Małe i duże litery, znaki alfanumeryczne, okresowe zmiany hasła
Etapy tworzenia zabezpieczeń – analiza wymagań, projektowanie, wdrożenie, zarządzanie
Szyfrowanie – zapis danych tak, żeby tylko uprawnieni mogli czytać
Kodowanie – zapis danych w taki sposób, żeby były dostępne dla wszystkich osób
Kryptologia – dziedzina wiedzy o przekazywaniu informacji tak ,żeby uchronić przed nieuprawnionym dostępem.
Szyfrogram – zaszyfrowana wiadomość
Klucz szyfrujący – dane służące do szyfrowania
Klucz deszyfrujący – dane służące do deszyfrowania
Klasyczne algorytmy szyfrujące – łatwe do złamania, samo algorytm musiał być chroniony
Algorytmy przestawieniowe – zmiana kolejności znaków zgodnie z wybraną figurą geometryczną
Algorytmy podstawieniowe:
Monoalfabetyczne – służą do zamiany pojedynczego znaku w konkretny znak szyfrogramu
Homofoniczne – każdy znak posiada własny zbiór symboli zwanych homonofonami.
Wieloalfabetowe – wiele niezależnych podstawień monoalfabetycznych.
Poligramowe – w 1 **k**roku jest szyfrowany więcej niż 1 znak

Algorytmy mieszane – wykorzystywanie wielu sposobów szyfrowania
Kryteria Shannona – ilość tajności zaoferowanej, rozmiar klucza, łatwość, propagacja błędów, powiększanie się wiadomości
Szyfry symetryczne – do szyfrowania danych
Algorytmy strumieniowe – do szyfrowania i deszyfrowania ten sam klucz, klucz na ciągu pseudolosowym
Algorytmy Blokowe – szyfrują bloki input w oparciu o zadany klucz
Asymetryczne – klucz tajny i jawny, tajny zna tylko właściciel, jawny powszechnie znany
Tryb pracy szyfrów blokowych – ECB, CBC, CFB
DES – symetryczny blokowy, 64 bit, klucz 56bit
3DES – używane 3 klucze, szyforwanie – 1, deszyfrowanie – 2, ponowne szyfrowanie – 3
IDEA – symetryczny blokowy, 64bit, klucz 128bit
AES – Rijndael – symetryczny blokowy, 128bit, 192bit, 256bit, klucz takie same rozmiary
Blowfish – asymetryczny blokowy, dane 64bit, klucz od 32 do 448bit,
RC5 – symetryczny blokowy, dane 32,64,128bit, klucz od 0 do 2040bit
RSA – asymetryczny, do szyfrowania i podpisów cyfrowych, faktoryzacja dużych liczb
Algorytm Deffiego-Hellmana – ustala klucz szyfrujący, szyfrowanie komunikacji
ElGamal - asymetryczny, do szyfrowania i obsługi podpisów cyfrowych
Funkcje skrótu – haszujące, mieszające, jednokierunkowe,
MD2 – losowe permutowanie bajtów, wada: szybkość działania, nie powinny być wykorzystywane
MD4 – skrót o długości 128bit, blok 512bitowy, 4 zmienne łańcuchowe
MD5 – ulepszone MD4, skrót 128bit, cztery cykle (64kroki)
SHA1- blok 512bit, skrót 160bit, bazuje na MD4, 4 cykle,
SHA2 – długość skrótu 224, 256, 384, 512, blok 512bit, 64rundy
SHA3 – algorytm Keccaka, wyższa wydajność niż SHA2, 24rundy, konstrukcja gąbki
Enigma - przenośna elektromechaniczna maszyna szyfrująca, oparta na zasadzie obracających się wirników, połączenie systemów elektrycznego i mechanicznego.
Skytale – metoda szyfrowania, na laske nawijano pasek pergaminu, a tekst pisano na stykających się brzegach.
Urząd certyfikacji:
Rodzaje certyfikacji – wewnętrzna/zewnętrzna
Model hierarchiczny – poziom emitujący powinien być weryfikowany przez nasz poziom pośredni, emitujący to konkretna osoba, która wystawia certyfikat
Centra certyfikujące – komercyjne, polska komercyjne, niekomercyjne