Podjela sigurnosnih mehanizama:

- ZAŠTITA OD VANJSKIH UTJECAJA
- ZAŠTITA OSTVARENA SUČELJEM PREMA KORISNIKU
    - identifikacija (predstavljanje), autentifikacija (provjera identifikacije)
- UNUTARNJI ZAŠTITNI MEHANIZMI
    - autorizacija (dopuštanje pristupa)
        - SUBJEKT = pojedini korisnik (ili njegov proces ili dretva)
        - OBJEKT = sredstvo koje se zaštićuje
        - ZAŠTITNA PRAVILA za svaki par subjekt-objekt određuju pravo pristupa
- KOMUNIKACIJSKI ZAŠTITNI MEHANIZMI
    - kriptiranje

Vrste napada na sigurnost:

- PRISLUŠKIVANJE (presretanje)
    - pasivni napad
    - djeluje na povjerljivost, odnosno tajnost
- PREKIDANJE
    - narušava raspoloživost
- PROMJENA SADRŽAJA PORUKA
    - narušava besprijekornost ili integritet
- IZMIŠLJANJE PORUKA
    - narušava besprijekornost ili integritet
- LAŽNO PREDSTAVLJANJE
- PORICANJE

Sigurnosni zahtjevi (prva 3 su osnovna):

- POVJERLJIVOST (TAJNOST)
    - informacije u sustavu smiju biti pristupačne samo ovlaštenim korisnicima
- RASPOLOŽIVOST
    - informacije moraju uvijek biti na raspolaganju ovlaštenim korisnicima
- BESPRIJEKORNOST
    - informacije u sustavu mogu mijenjati samo za to ovlašteni korisnici
- AUTENTIČNOST
    - ovlašteni se korisnici moraju jednoznačno moći prepoznati
- AUTORIZACIJA
    - ovlaštenim se korisnicima postupkom autorizacije dopušta pristup samo do nekih sadržaja
- NEPORECIVOST
    - zaštita od opovrgavanja, neporicanje

Utjecaj pojedinih komponenti računalnih sustava na sigurnost:

- SKLOPOVLJE RAČUNALA
  - utječe na raspoloživost informacija
  - podložno vanjskim utjecajima
  - korištenje zalihosti za povećanje raspoloživosti
- PROGRAMI
  - utječu na tajnost, besprijekornost i raspoloživost
  - VIRUS = programski odsječak koji se komunikacijom ili razmjenom spremničkih medija unosi u računalni sustav
  - preventivno djelovanje protiv virusa
  - CRV = cjeloviti program koji sam sebe kroz komunikacijsku mrežu prenosi s jednog računala na drugi, pri čemu djeluje destruktivno
  - TROJANSKI KONJ = program koji obavlja neki koristan posao, ali mu je pridodana neka funkcija koja štetno djeluje
- PODACI
  - podložni narušavanju raspoloživosti, tajnosti i besprijekornosti
  - povećanje sigurnosti kontrolom pristupa
- KOMUNIKACIJE
  - podložne narušavanju raspoloživosti, tajnosti i besprijekornosti
  - najosjetljiviji dio računalnih sustava

Svi sigurnosti zahtjevi osim raspoloživosti mogu se zadovoljiti KRIPTIRANJEM SADRŽAJA.

RAZGOVJETNI (JASNI) TEKST = izvorni oblik podataka

KRIPTIRANJE = postupak prevođenja jasnog teksta u KRIPTIRANI TEKST

DEKRIPTIRANJE = postupak prevođenja kriptiranog teksta u jasni tekst

Današnji kriptografski sustavi su parametarske matematičke funkcije, odnosno algoritmi, kojima se nizovi bitova jasnog teksta preračunavaju u nizove bitova kriptiranog teksta i obrnuto.

FUNKCIJA KRIPTIRANJA : $\mathbf{C = E(P, K_E)}$

P = jasni tekst

C = kriptirani tekst

E = funkcija kriptiranja

K_E = parametar ili ključ kriptiranja

FUNKCIJA DEKRIPTIRANJA: $\mathbf{P = D(C, K_D)}$

D = funkcija dekriptiranja

K_D = parametar ili ključ dekriptiranja

Funkcija dekriptiranja mora biti inverzna funkciji kriptiranja: **$P = D(E(P, K_E), K_D)$**

KRIPTOSUSTAV = funkcije kriptiranja E i dekriptiranja D

NESIGURNI KOMUNIKACIJSKI KANAL = komunikacijski kanal koji nije zaštićen, preko njega se prenosi kriptirana poruka

POVJERLJIVI KOMUNIKACIJSKI KANAL = kanal koji nastaje postupcima kriptiranja i dekriptiranja između izvorišta koje je kriptiralo podatke koje šalje i odredišta koje je primljene podatke dekriptiralo

Današnji kriptosustavi zasnivaju se na postupcima koji se efikasno mogu izvoditi na računalima, a ti postupci zasnivaju se na algoritmima koji su u pravilu opće poznati, ali s ključevima koji imaju vrlo velik broj mogućih vrijednosti.

Dobrota kriptosustava određena je težinom otkrivanja ključa dekriptiranja.

Danas su u uporabi dva osnovna oblika kriptosustava:

- SIMETRIČNI KRIPTOSUSTAVI
  - ključ kriptiranja jednak je ključu dekriptiranja (ključ K)
  - $C = E(P, K)$
  - $P = D(C, K)$
  - $P = D(E(P, K), K)$
- ASIMETRIČNI KRIPTOSUSTAVI
  - ključ kriptiranja (K_E) i dekriptiranja (K_D) su različiti
  - $C = E(P, K_E)$
  - $P = D(C, K_D)$
  - $P = D(E(P, K_E), K_D)$

DATA ENCRYPTION SYSTEM (DES):

- zasniva se na permutaciji bitova i operaciji XOR
- kriptiraju se blokovi duljine 64 bita
- ključ kriptiranja ima 56 bitova i iz njega se određuje 16 parametara (podključeva)
- opis postupka:
  - permutiranje jednog bloka jasnog teksta, a rezultat se dijeli na dvije polovine (L_0R_0)
  - u 16 koraka obavlja se manipulacija bitovima (i = 1, 2, …, 16)
    - $L_i = R_{i-1}$
    - $R_i = L_{i-1}$ XOR $f(R_{i-1}, K_i)$
    - funkcija f obavlja preslagivanje bitova, ovisno o ključu
  - na kraju se obavlja inverzna permutacija
    - $C = IP^{-1}(L_{16}R_{16})$

UTROSTRUČENI DES (3DES)

- umjesto jednog ključa upotrebljavaju se 3 ključa
- **$3DES(P, K_1, K_2, K_3) = DES(DES^{-1}(DES(P, K_1), K_2), K_3)$**
- **$3DES^{-1}(C, K_1, K_2, K_3) = DES^{-1}(DES(DES^{-1}(C, K_3), K_2), K_1)$**

IZBIJELJENI DES (DESX)

- u osnovni 56-bitnu ključ (K_1) koriste se još dva 64-bitna ključa za „izbjeljivanje" teksta (K_2 i K_3)
- **$DESX(P, K_1, K_2, K_3) = DES(P \text{ xor } K_2, K_1) \text{ xor } K_3$**
- **$DESX^{-1}(C, K_1, K_2, K_3) = DES^{-1}(C \text{ xor } K_3, K_1) \text{ xor } K_2$**

KRIPTOSUSTAV IDEA

- kriptiraju se blokovi 64 bita
- pri kriptiranju se blokovi dijele u 4 podbloka od 16 bitova
- ključ ima 128 bita, a iz njega je potrebno odrediti 52 podključa duljine 16 bita
- algoritam se provodi u 9 koraka
    - u prvih 8 koraka s 4 podbloka i 6 podključeva obavljaju se sljedeće operacije
        - XOR
        - zbrajanje po modulu 2^{16}
        - množenje po modulu $2^{16} + 1$
    - u devetom koraku upotrebljavaju se 4 podključa i ne koristi se xor
- dvostruko brže od DES-a

ADVANCED ENCRYPTION SYSTEM (AES)

- simetrični blok algoritam s javnim izvornim tekstom programa
- blok podataka koji se kriptira minimalne je veličine 128 bita
- veličina ključa od 128, 192 i 256 bita
- koristi konačno polje $GF(2^8)$, nad kojim su definirane operacije zbrajanja i množenja
    - zbrajanje = xor
    - množenje polinoma stupnja 8 je zapravo binarno množenje polinoma modulo fiksni ireducibilni polinom $g(x) = x^8 + x^4 + x^3 + x + 1$
    - u slučaju množenja polinoma stupnja manjeg od 4, množenje dvaju polinoma definirano je kao binarno množenje polinoma modulo polinom $x^4 + 1$
- pobjednik natječaja za AES bio je RIJNDAEL
    - promjenjive duljine bloka teksta i ključa (128, 192 ili 256)
    - blok koji se kriptira smješten je u pravokutni niz bajtova u 4 retka, a broj stupaca ovisi o duljini bloka pa može biti 4, 6 ili 8 (oznaka N_b), a na isti način se tretira i ključ pri čemu se broj stupaca označava s N_k
    - kriptiranje i dekriptiranje obavljaju se u koracima, a broj koraka N_r ovisi o N_b i N_k
        - $N_b = N_k = 4 \Rightarrow N_r = 10$
        - $N_b = 6$ ili $N_k = 6 \Rightarrow N_r = 12$, a inače 14
    - u svakom koraku obavljaju se 4 transformacije:

- Zamijeni znakove
  - mijenja znak po znak koristeći supstitucijsku tablicu
- Posmakni redove
  - rotira znakove udesno, i to u drugom,trećem i četvrtom retku bloka za unaprijed poznati broj mjesta koji ovisi o N_b
- Pomiješaj stupce (ne obavlja se jedino u zadnjem koraku)
  - množi se stupac po stupac bloka (svaki stupac se promatra kao četveročlani polinom) s fiksnim polinomom $a(x) = 03_H x^3 + 01_h x^2 + 01_h x + 02_h$ modulo $x^4 + 1$
- Dodaj podključ

- podključevi su po veličini jednaki veličini bloka koji se kriptira i dobivaju se iz izvornog ključa, a zajedno čine prošireni ključ
  - prošireni ključ dobiva kopiranjem izvornog na početak proširenog, a ostatak se gradi korištenjem xor, rotacije bitova, zamjene bajtova uz pomoć supstitucijskih tablica te dodavanjem konstanti
  - prošireni ključ ima $(N_r + 1) * N_b$ bitova

Načini kriptiranja:

- ELECTRONIC CODEBOOK (ECB)
  - najjednostavniji, uobičajeni
  - svaki blok se kriptira (i dekriptira) zasebno
  - svojstva:
    - identični slijedni nekriptirani blokovi rezultiraju identičnim kriptiranim blokovima
    - blokovi su kriptirani nezavisno o ostalim blokovima
    - pogreška unutar jednog bloka utječe na dešifriranje samo tog bloka
- CIPHER BLOCK CHAINING (CBC)
  - najpopularniji način rada za kriptiranje blokova jasnog teksta
  - jasni tekst se zbraja (xor) s kriptiranim blokom i tada se primjenjuje algoritam na rezultirajući blok (u prvom koraku se zbraja inicijalizacijski vektor s jasnim tekstom)
  - svojstva:
    - blok kriptiranog teksta ovisi o svim prethodnim blokovima
    - povećanje razine sigurnosti postiže se izbjegavanjem korištenja istog inicijalizacijskog vektora s istim ključem
    - zbog ulančavanja kriptirani blok c_j ovisi o x_j i svim nekriptiranim blokovima koji su prethodili
    - jedan bit pogreške u kriptiranom bloku c_j utječe na dekriptiranje blokova c_j i $c_j + 1$,
    - SAMOSINKRONIZIRAJUĆI način rada – kada se pojavi greška u nekom bloku c_j, ali ne i u $c_j + 1$, blok $c_j + 2$ je ispravno dekriptiran u $x_j + 2$, a isto vrijedi u slučaju gubitka jednog ili više blokova

- CIPHER FEEDBACK (CFB) i OUTPUT FEEDBACK (OFB)
    - za kriptiranje toka podataka, duljina ključa jednaka duljini poruke koja se kriptira
    - ključ proizvoljne duljine postiže se uzastopnim kriptiranjem neke početne vrijednosti (OFB) ili ulančanim kriptiranjem već kriptiranih blokova (CFB)
    - kriptirani tekst dobiva se zbrajanjem (xor) jasnog teksta s ključem koji je jednake duljine
    - inicijalizacijski vektor ne mora biti tajan
    - u CFB načinu pogreška se propagira do kraja dekriptiranja pa je tekst od mjesta pogreške izgubljen
    - kod OFB načina sljedeći kriptirani blok ne zavisi od prethodnog
- CTR NAČIN KRIPTIRANJA
    - sličan OFB i CFB
    - ključ se dobiva uzastopnim kriptiranjem rastuće vrijednosti brojača
    - umjesto brojača može se koristiti i neka druga funkcija koja ne ponavlja vrijednosti kroz duži period

---

DJELJIVOST

- broj a djeljiv je s brojem d kada je a višekratnik od d
- trivijalni djelitelji od a su 1 i a, a netrivijalni su svi ostali koji se nazivaju faktori

PROSTI (PRIM) BROJEVI

- broj a > 1 koji nema faktora je prosti broj

TEOREM DIJELJENJA

- za svaki cijeli broj a i bilo koji pozitivni cijeli broj n postoje jedinstveni cijeli brojevi za koje vrijedi **a = q*n + r**
    - q je količnik (kvocijent)
    - r je ostatak (reziduum), uz 0 <= r < n

EKVIVALENTNOST PO MODULU (KONGRUENTNOST)

- broj a jednak je broju b po modulu n ako je **a mod n = b mod n**
    - kaže se da su a i b kongruentni po modulu n i piše se a Ξ b (mod n)

RELATIVNO PROSTI BROJEVI

- brojevi a i b su relativno prosti brojevi ako im je najveći zajednički djelitelj 1

EULEROVA PHI FUNKCIJA

- Z_n ={ 0, 1, 2, …, n-1 } je prsten u kojem su definirane operacije zbrajanja, oduzimanja i množenja po modulu n
- Z_n* je podskup Z_n koji se sastoji od elemenata koji su relativno prosti u odnosu na n
- broj elemenata skupa Z_n* jednak je Eulerovoj phi ili totient funkciji **j(n)**
- n = p (prosti broj) =>j(p) = p – 1
- n = pq (p i q su prosti brojevi) => j(n) = (p-1)(q-1)

EULEROV TEOREM

- za svaki prirodni broj n > 1 vrijedi za sve brojeve a iz skupa Z_n*
  $a^{j(n)} \equiv 1 \pmod n$

MALI FERMATOV TEOREM

- za proste brojeve p vrijedi za svaki broj a iz skupa Z_n*
  $a^{p-1} \equiv 1 \pmod p$
- **$a^{p} \equiv a \pmod p$**

ASIMETRIČNI KRIPTOSUSTAV RSA

- postupak izgradnje RSA sustava:
  - odabiru se dva velika prosta broja p i q ($p > 10^{100}$, $q > 10^{100}$)
  - izračuna se umnožak n = pq
  - izračuna se umnožak $\phi(n) = (p-1)(q-1)$
  - odabire se broj $e < \phi(n)$ i relativno prost u odnosu na $\phi(n)$
  - izračunava se broj $d < \phi(n)$ tako da bude umnožak $ed = 1 \pmod{\phi(n)}$
  - par $K_E = (e, n)$ obznanjuje se i proglašava javnim ključem
  - par $K_D = (d, n)$ se taji postaje privatni ključ
- kriptiranje: **$RSA\ (P, K_E) = P^e \bmod n$**
- dekriptiranje: **$RSA^{-1}\ (P, K_D) = C^d \bmod n$**
- tajnost se postiže odabirom prostih brojeva s velikim brojem dekadskih znamenki
- nekoliko redova veličina sporije u odnosu na simetrične kriptosustave

---

DIGITALNA OMOTNICA

- postupak stvaranja digitalne omotnice M:
  - odabir proizvoljnog simetričnog ključa K
  - kriptiranje teksta P simetričnom funkcijom, primjerice DES – **$C_1 = DES(P, K)$**
  - kriptiranje tajnog ključa javnim ključem sugovornika – **$C_2 = RSA(K, K_E)$**
  - slanje poruke **$M = (C_1, C_2)$**
- postupak dekriptiranja:
  - dekriptiranje C_2 privatnim ključem ne bi li se saznao simetrični ključ – **$K = RSA^{-1}\ (C_2, K_D)$**
  - dekriptiranje C_1 upravo saznatim ključem – **$P = DES^{-1}\ (C_1, K)$**
- osigurava tajnost poruke, ali ne i ostale sigurnosne zahtjeve

---

```
funkcija provjera_složenosti (a, n, G) {
      G = 0;
      d = 1;
      c = n - 1;
      i = -1;

      dok je c > 0 {
            i++;
            b[i] = c mod 2;
            c = c div 2;
      }

      dok je ((i >= 0) ∧ (G == 0)) {
            d_s = d;
            d = (d * d) mod n;
            ako je ((d == 1) ∧ (d_s != 1) ∧ (d_s != n-1)) {
                  G = 1;
            }
            ako je (b[i] == 1) {
                  d = (d*a) mod n;
            }
            i--;
      }

      ako je ((i == -1) ∧ (d != 1)) {
            G = 1;
      }
}
```

PROGRAM KOJI ODREĐUJE JE LI BROJ SLOŽEN (random vraća nasumični broj veći od 1 i manji od n-1):

```
G = 0;
i = k;
dok je ((i >= 0) ∧ (G == 0)) {
      a = random (1, n-1);
      provjera_složenosti(a, n, G);
      i--;
}
ako je (G == 1) {
      n je složeni broj     // sigurno!
}
inače {
      n je prosti broj      // skoro sigurno!
}
```

NAPADI NA KRIPTOSUSTAVE

- vrste napada prema onome što je napadaču dostupno
    - NAPAD S ODABRANIM ČISTIM TEKSTOM
        - neograničene količine parova (M, C)
    - NAPAD S ODABRANIM KRIPTIRANIM TEKSTOM
        - po volji odabrani C i pripadni M (neograničene količine)
    - NAPAD S POZNATIM ČISTIM TEKSTOM
        - neki parovi (M, C)
    - NAPAD S POZNATIM KRIPTIRANIM TEKSTOM
        - dostupan samo C, a traži se K i M
- PRETRAŽIVANJE CIJELOG PROSTORA RJEŠENJA
    - isprobavaju se svi mogući ključevi
    - najjednostavnija i najsporija vrsta napada
    - nije moguće spriječiti
    - napad koji ima veću složenost od složenosti pretraživanja cijelog prostora smatra se neuspješnim
    - napadač ili ima na raspolaganju čisti tekst ili pretpostavlja da čisti tekst ima neku strukturu koju je moguće prepoznati
- PRETRAŽIVANJE POLA PROSTORA RJEŠENJA
    - kod mnogih kriptosustava za koje vrijedi simetrija:
        - C = DES (M, K), C' = DES (M',K'), gdje je X'oznaka za bitovni komplement
    - ušteda je blizu 50%
    - vrijedi i za DES
- pomoć u napadu na kriptosustave: uzeti u obzir frekvenciju slova
- NAPADI NA DES
    - DES bitno oslabljuje:
        - promjena redoslijeda S tablica
        - slučajno odabrane S tablice
        - umjesto xor neka složenija funkcija
    - pristup: ANALIZA POJEDNOSTAVLJENOG KRIPTOSUSTAVA
        - s manje iteracija ili rundi
- DIFERENCIJALNA KRIPTOANALIZA
    - tehnika kojom se analizira učinak razlike između dva čista teksta na razliku između dva rezultirajuća kriptirana teksta
    - napad s odabranim/poznatim čistim tekstom
- LINEARNA KRIPTOANALIZA
    - cilj je pronaći linearnu aproksimaciju danog algoritma
    - aproksimacija nikada nema vjerojatnost ni blizu 100%, što se nadoknađuje uzimanjem veće količine parova čisti – kriptirani tekst
    - obično više linearnih aproksimacija za neki algoritam
    - učinkovitost algoritma raste s $|p – 0,5|$ i s rastom broja poznatih tekstova
    - DES je moguće brže probiti od pretraživanja cijelog cijelog prostora