

Securitate

- Criterii:
- confidențialitate (datele): cîndă doar în unele cazuri.
 - (funcționalități) → integritate (datele să nu fie citite și modificate): cîndă.
 - accesibilitate (cine are dreptul să modifice datele să poată și le modifice)

• Funcționalitățile trebuie îndeplinite toate pentru a avea o securitate bună.

* CriptografieAlgoritmi:

- RSA: - bazat pe chei publice și chei private.
 - utilizatorul folosește un program care generează două chei
 - toate lumea știe cheia publică dar nu și cea privată
 - textul se decriptează folosind cheia privată

$$A \xrightarrow{f} B \xrightarrow{g} A \quad fg(gf) = 1$$

identitatea

• SSH, SETP - bazate pe RSA

- Chei fluide: - pentru comunicații
 - din 10 în 10 sec. se schimbă cheia

- RC4: - pentru comunicații online

Examen 8

- Media : $(\text{lab} + \text{sens} + \text{oral} + \text{total}) / 4$
 - Oral : - două subiecte (ex. regulile de securitate)
 - Teste 8 de serie : se poate renunța la oral : $(\text{lab} + 3 \cdot \text{sens}) / 4$
 - Lucrarea senșii : > 5
 - 6 întrebări : 1 pct (max 2 răsulturi rezolvare)
 - arh multi-procesor , perferen care permite
- scrierea unui fișier etc.
- 2 probleme de programare (ex C) - programare avansată
- funcții , sau programe (ex. scrieți o funcție ... care face ... returnează ---) → problemele cu fișiere sunt favorite

Ex :

1) ind myfnct (char* f1, char* f2) // mișcarea unor fișiere

```

{
    FILE *fp1, *fp2; // de testat costul de retur al lui fopen
    char x;
    if ((fp1 = fopen(f1, "r")) == NULL) // nu folosim not
        return -1; // se compară cu NULL
    if ((fp2 = fopen(f2, "w")) == NULL)
    {
        return -1;
        fclose(fp1);
        return -1;
    }
    while (x = fgetc(fp1) != EOF)
        if (fputc(x, fp2) == EOF)
        {
            fclose(fp1);
            fclose(fp2);
            return -1;
        }
}

```

- func care copiază fi în fi.
- return 0 → succes
- -1 → eșec

```
fclose(fp1);  
fclose(fp2);  
return 0;  
}
```

2) Scrieți o funcție în care numele fișierelor să nu fie clar
ca descriptori (unul deschis) (indicați)
nu se mai include

- Să nu se folosească variabile globale decât dacă sunt menționate în enunț

- Materiale: foaie A4 + cartă