Probleme ce trebuiesc rezolvate la Securitate software.
Cifruri prin supozitie (schimbarea literelor alfabetului cu literele unui alt alfabet sau alte simboluri)

1. Cifrul Cezar pe fisier atat criptare cat si decriptare
2. Cifrul cezar imbunatatit prin folosirea unui alphabet cu literele deplasate (shiftate) la fiecare nou pas, adica pt fiecare character nou al textului clar
3. Derivata din cifrul Cezar cu 10 alfabete amestecate si pt fiecare character al textului clar se foloseste complementara dintr-un alt alfabet . Alfabetele complementare pot fi generate aleator, in acest caz si seed-ul generatorului d enr aleatoare este un secret.

Cifruri prin transpozitie

1. Citirea pe sarite a unui text. Pasul cu care sunt citite literele textului este secretul
2. Aceeasi problema doar ca pasul este variabil, adica distanta dintre diferitele litere citite din text se modifica la fiecare noua litera

Cifruri binare cu operatii logice

1. Transformarea caracterului in nr binar fara a se folosi functii predefinite ale limbajelor de programare (atentie, „numarul” binar va trebuii salvat ca si text). Operatia inversa adica un nr binar transformat in caracterul ASCII corespunzator
2. Criptare cu XOR. Literele textului clar si ale cheii sunt convertite in binar apoi bitii acestor numere binare sunt combinate prin XOR pentru a obtine textul cifrat.
3. Algoritm pentru extinderea cheii.

Aplicatii comerciale. HASH, md5,
Semnatura digitala, autentificarea unui document digital: Concepeti o aplicatie care sa realizeze rezumatul criptat al unui text.

Criptografia vizuala. Realizati un program care sa cripteze o imagine bmp prin XOR Se citeste fiecare pixel al imaginii. Codul de culoare al pixelului este criptat XOR cu bitii unei chei. Se afiseaza/salveaza imaginea astfel obtinuta. Utilitate CAPTCHA suplimentar adica pe langa faptul ca o aplicatie vrea dovada ca este vb de un utilizatro uman, acesta mai este si testat prin afisarea uni captcha cripta. Pentru a raspunde la provocare utilizatorul trebuie mai intai sa decripteze imaginea pentru a o interpreta si apoi raspunde provocarii.