

# Projektförslag

Erwin Hörnell  
erho.6814

Leonard Öhrström  
leoh.3739

27 oktober 2025

# 1 Vår idé

Vår idé är ett textkrypteringsprogram som kan kryptera och dekryptera hela textfiler. Kryptering är ett viktigt verktyg för att bekämpa cyberattacker riktade mot känslig data. Genom att använda programmet blir användarens data mer säker.

## 2 Systemets delar

Systemet består av två huvuddelar, viktigaste delen är en modul för att kryptera text och filer med hjälp av en symmetrisk nyckel. Nyckeln är en sträng genererad av programmet med hjälp av ett lösenord, den används både för att kryptera och sedan dekryptera. Denna del krypterar med två olika algoritmer, vigenère chiffer och XOR chiffer.

Den andra delen av programmet är en text baserad interface för användare att först välja lösenord och sedan välja filer som ska behandlas.

## 3 Representation

Okrypterad text: sträng

Krypterad text: sträng

Lösenord: sträng

Slumptal: sträng

Salt: sträng

Saltat lösenord: sträng

## 4 Komplexitet och förenkling

Till att börja med behöver funktioner för kryptering och avkryptering skapas, samt funktion för att generera saltat lösenord. Därefter behövs ett front end-system för att hantera användarinput. Detta bör först utvecklas för terminal, därefter om möjligt vidareutvecklas med hjälp av ett separat GUI-bibliotek.

## 5 Personliga utvecklingsmål

### 5.1 Erwin mål

Jag vill ägna mer tid åt planering och abstrahering innan någon kodning sker för att lättare kunna utveckla olika system samtidigt oberoende av varandra. Ett sätt vi tänker förverkliga detta är att använda funktion hints och platshållar retur

värden. På så sätt kan vi använda funktioner som inte är klara än vilket låter oss jobba oberoende av varandra.

## **5.2 Leonard mål**

Jag vill utveckla min förmåga att bryta ner problem till stegvis mindre problem vars lösningar slutligen kan sättas ihop för att lösa ursprungsproblemet (söndra och härska). Jag tror detta främst kräver övning och erfarenhet. Detta mål passar även bra med Erwins, då båda berör funktioner och abstraktion. För att ta hänsyn till detta mål kommer vi till viss del planera programmets struktur innan, samt så kommer jag vara noggrann med att alltid fundera över hur jag arbetar med funktioner under projektet.