SecureVault

Password Manager

—

תמר אביטן - דרכי חנה

SecureVault

Modern Password Management

מבוא

אלגוריתמי הצפנה קיימים

תיאור הפרויקט:

אלגוריתם הצפנה המבוסס על תורת הגרפים

מנהל סיסמאות כמעטפת

SecureVault

Modern Password Management

הבעיה האלגוריתמית

- הצפנה מתקדמת באמצעות אלגוריתם מאובטח

SecureVault

Modern Password Management

אלגוריתם הפתרון

- הצפנה סימטרית המבוססת על מעגלים המילטוניים בגרף
- שימוש ב- CBC mode ומחולל BBS למפתחות

SecureVault

Modern Password Management

נימוקים לבחירת האלגוריתם

- שילוב ייחודי של תורת הגרפים עם קריפטוגרפיה
- BBS
- CBC

- השילוב הייחודי של תורת הגרפים עם קריפטוגרפיה יוצר מורכבות מתמטית.
- כל סיסמה מוצפנת עם מפתח אחר

SecureVault

Modern Password Management

- טיפול בסיסמא

סיסמה לדוגמא : myPass12@&^l

אורך הסיסמה: 12

המרה לאסקי

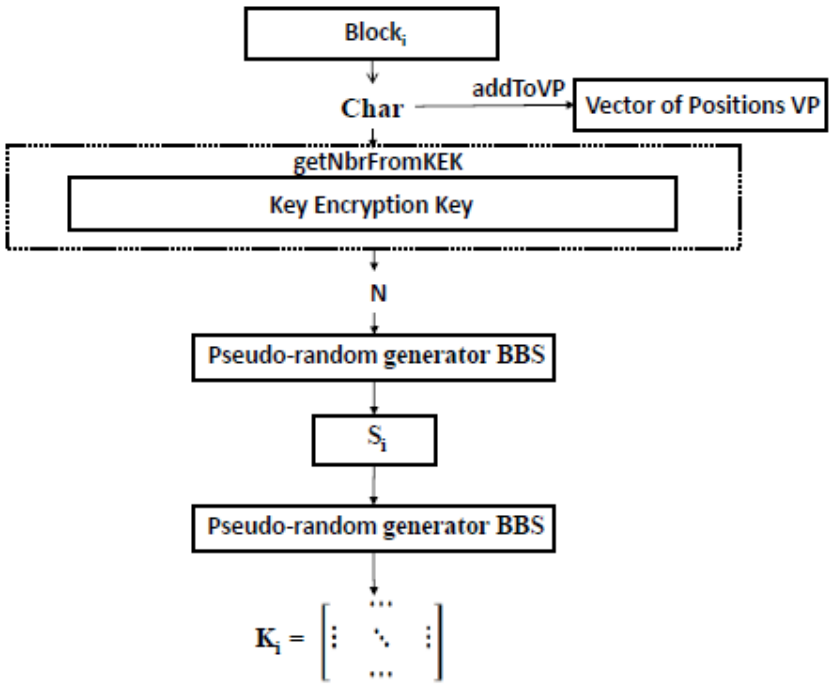
0	1	2	..	..										12	...					..					...				77
1	2	m	y	p	a	s	s	1	2	@	&	^	l	....				F				h	y	d	L	f	k	i	h

SecureVault

Modern Password Management

יצירת מפתחות הצפנה

- מפתח מאסטר
- מטריצת אתחול

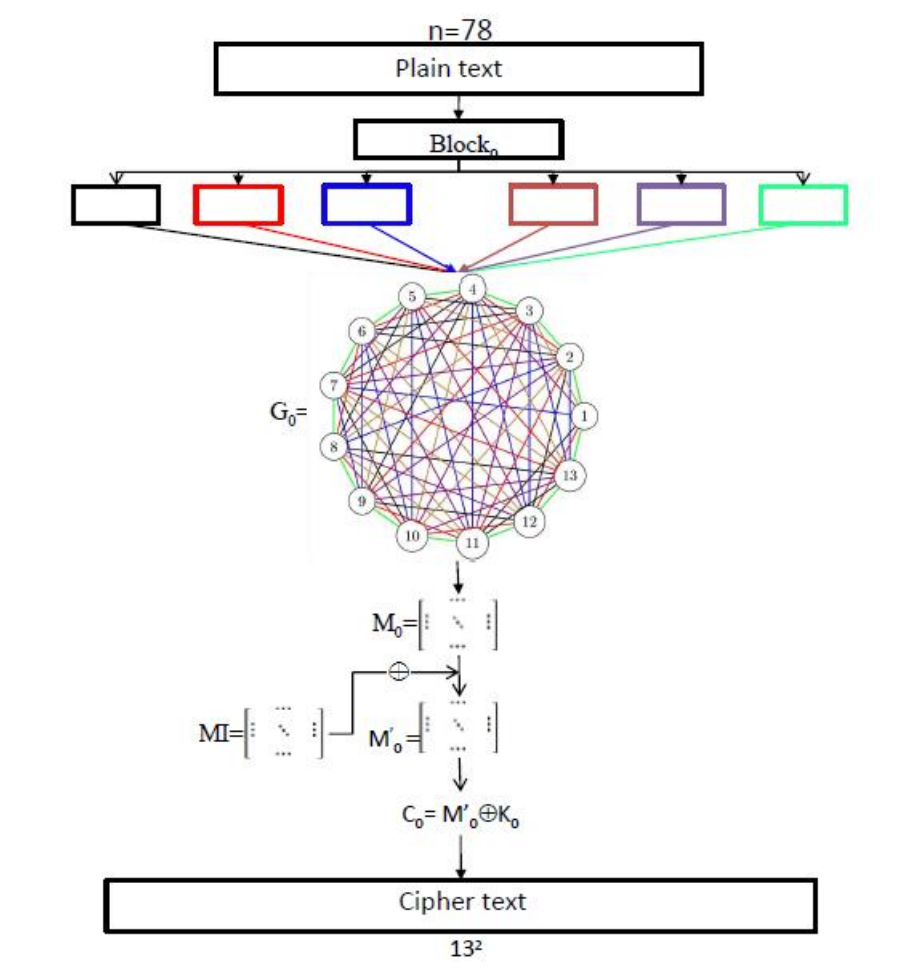


SecureVault

Modern Password Management

המשך תהליך האלגוריתם

הצפנה.

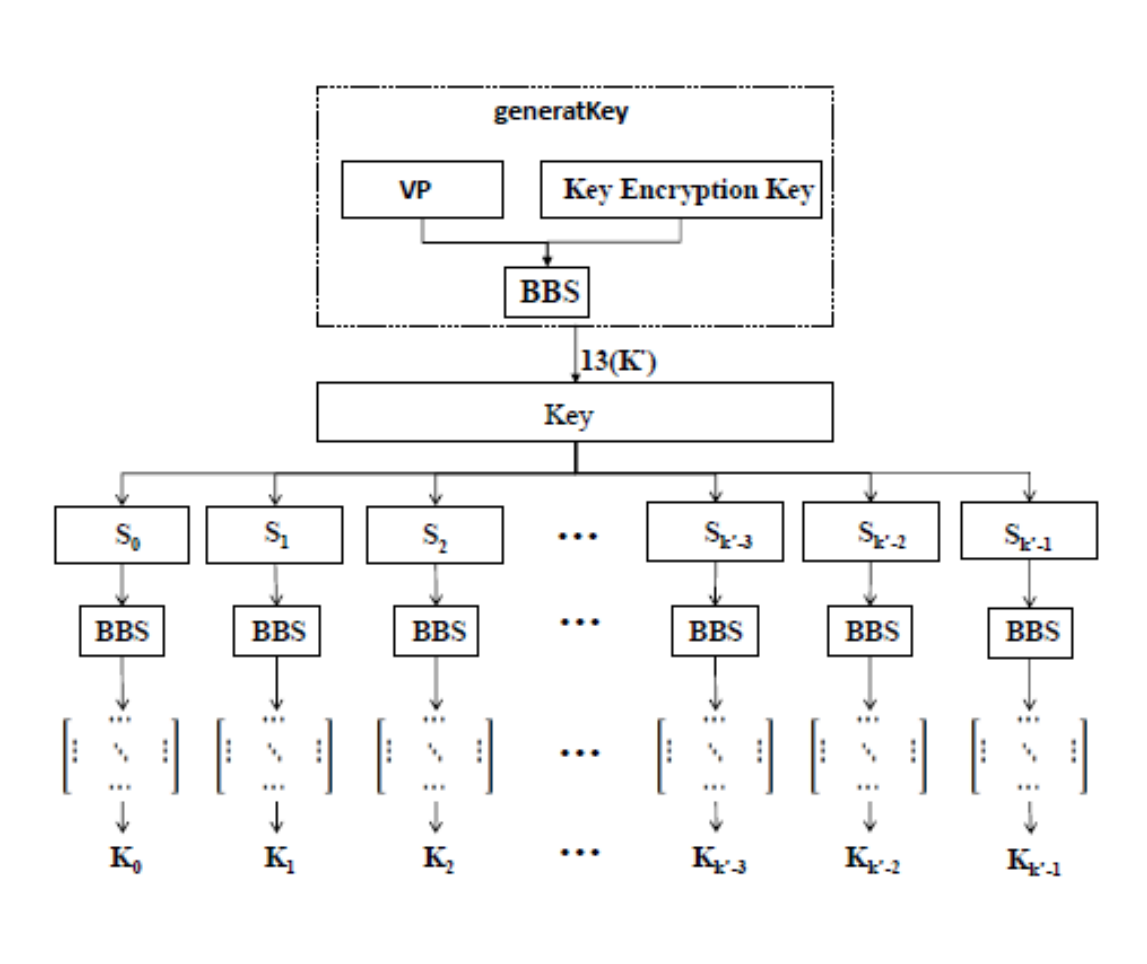


SecureVault

Modern Password Management

פענוח

יצירת מפתחות



SecureVault

Modern Password Management

סקירת חלופות טכנולוגיות וסביבות עבודה

- NET Core vs.
- Java Spring vs
- Python Flask

- MongoDB vs SQL Server vs PostgreSQL

SecureVault

Modern Password Management

טכנולוגיה נבחרת

- NET Core 8: ביצועים גבוהים, אבטחה מובנית, ארכיטקטורת שכבות
- MongoDB: גמישות בשמירת נתונים, ביצועים טובים.

SecureVault

Modern Password Management

ארכיטקטורת המערכת

- שכבת API (Controllers),
- שכבת BL (Business Logic),
- שכבת DAL – גישה למסד הנתונים

SecureVault

Modern Password Management

תודה רבה

—