

Proposal for Translating Cryptology Terms to Hebrew

Yossi Markovitz initiated this list. Ron Irmay, Shraga Irmay, Adi Shamir, Moti Yung, Orr Dunkelman and Roni Roth contributed various terms and had various suggestions that improved this list. Some translations were adopted from the Israeli electronic signature law, 2001.

General Terms

Cryptography _____ (כתיבת סתר, קריפטוגרפיה)
Cryptology _____ (קריפטולוגיה) תורת הצפנים
Cryptanalysis _____ קריפטאנליזה
Cryptographer _____ (על משקל גנן) צפן
Cryptanalyst _____ (גלאי?) קריפטאנליסט
Encryption _____ הצפנה
Decryption _____ פננוח
Cipher _____ צופן
Cryptosystem _____ מערכת הצפנה
Plaintext _____ כתב גלוי
Ciphertext _____ כתב סתר
Key _____ מפתח
Password _____ סיסמא
One-Time Pad _____ מפתח חד-פעמי
Key Distribution, Key Exchange _____ (החלפת מפתחות) הפצת מפתחות
Key space _____ מרחב מפתחות

Types of Attacks

Attack _____ התקפה
Ciphertext Only Attack _____ התקפת כתב סתר בלבד
Known Plaintext Attack _____ התקפת כתב גלוי ידוע
Chosen Plaintext Attack _____ התקפת כתב גלוי נבחר
Adaptive Attack _____ התקפה מסתגלת
Chosen Key Attack _____ התקפת מפתח נבחר
Exhaustive Search Attack _____ התקפת חפוש ממצה
Dictionary Attack _____ התקפת מילון
Meet in the Middle Attack _____ התקפת פגישה באמצע

Symmetric Ciphers Terms

Block Cipher _____ צופן בלוקים
Stream Cipher _____ צופן שטף
Round _____ שלב
Key Schedule _____ עבוד מפתחות
Subkey _____ מפתח תת-צופן
Weak Key _____ מפתח חלש
Double Encryption _____ דו-צופן
Triple Encryption _____ תלת-צופן
Mode of Operation _____ מוד תפעול, (ארץ תפעול)
Differential Cryptanalysis _____ קריפטאנליזה דיפרנציאלית
Linear Cryptanalysis _____ קריפטאנליזה ליניארית
Characteristic _____ תכונה
Differential _____ דיפרנציאל
Linear Feedback Shift Register _____ אגור הזזה עם משוב ליניארי

Hashing Terms

Hash Function _____ (ערבול זה scrambling) פונקציית תמצות
One Way Function _____ פונקציה חד-כוונית
One Way Hash Function _____ פונקציית תמצות חד-כוונית
Hash Value _____ תמצית
Message Authentication Code _____ קוד אמרת הודעות
Birthday Paradox _____ פרדוקס יום ההולדת
Birthday Attack _____ התקפת יום הולדת
Collision _____ התנגשות
Collision Free Hash Function _____ פונקציית תמצות ללא התנגשויות
Compression Function _____ פונקציית דחיסה
Padding _____ ריפוד

Public Key Terms

Public Key Cryptography _____ צפנות מפתח פומבי
Public Key _____ מפתח פומבי (צבורי)
למעשה המפתח אינו צבורי, הוא מפורסם בפומבי אך יש לו בעלים מסוים.
Secret (Private) Key _____ מפתח סודי (פרטי)
Digital Signature _____ חתימה אלקטרונית, חתימה ספרתית
Authentication _____ אמות
Identification _____ זהו
Public Key Infrastructure _____ תשתית מפתח פומבי
Certificate _____ תעודה אלקטרונית, אישור
Certification Authority _____ גורם מאשר, רשות מאשרת
Certificate Revocation List _____ רשימת בטולי אשורים
Quadratic Sieve _____ נפה רבועית
Trapdoor One-Way Function _____ פונקציה חד-כוונית עם דלת מלכודת

Number Theory Terms

Number Theory _____ תורת המספרים
Factoring _____ פירוק
Factor _____ גורם
Prime Factor _____ גורם ראשוני
Discrete Logarithm _____ לגריתם דיסקרטי
Modulus _____ מודולוס
Modular Arithmetic _____ חשבון מודולרי
Exponent _____ מעריך

Zero Knowledge Terms

Zero Knowledge Proof _____ הוכחת אפס ידע
Interactive Proof _____ הוכחה אינטראקטיבית
Zero Knowledge Interactive Proof _____ הוכחת אפס ידע אינטראקטיבית

Secret Sharing Terms

Secret Sharing _____ (חלוקת סוד), שתוף סוד
Threshold Scheme _____ (סכמת סף)
Share _____ (חלק), שתף (SHETEUF)
Share Holder _____ שותף
Share _____ (Share) יכול להיות גם מניה (המתחלקת בשיתוף בין הרבה גורמים)
ורק רוב (או או בעלי מספר מוגדר מראש של מניות) יכול להעביר החלטה.

Other Terms

Digital Cash, Electronic Money _____ כסף ספרתי
Covert Channel, Subliminal Channel _____ ערוץ חסוי
Handshake _____ לחיצת ידיים
Impersonation _____ התחזות
Random Number _____ מספר אקראי
Pseudo-Random Number _____ מספר אקראי-לכאורה
Pseudo-Random Sequence _____ סדרה אקראית-לכאורה
Seed _____ זרעון
Information Theory _____ תורת המידע
Entropy _____ אנטרופיה
Trusted Center _____ מרכז אמין