Proposal for Translating Cryptology Terms to Hebrew

Yossi Markovitz initiated this list. Ron Irmai, Shraga Irmai, 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	צפנות, (כתיבת סתר, קריפטוגרפיה)
Cryptology	תורת הצפנים, (קריפטולוגיה)
Cryptanalysis	קריפטאנליזה
Cryptographer	צפן (על משקל גנן)
Cryptanalyst	קריפטאנליסט, (גלאי?)
Encryption	הצפנה
Decryption	פענוח
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	הפצת מפתחות, (החלפת 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	תת מפתח
Weak Key	מפתח חלש
Double Encryption	דו-צופן
Triple Encryption	תלת-צופן
Mode of Operation	מוד תפעול, (אופן תפעול)
Differential Cryptanalysis	קריפטאנליזה דיפרנציאלית
Linear Cryptanalysis	קריפטאנליזה לינארית
Characteristic	תכונה
Differential	דיפרנציאל
Linear Feedback Shift Register	אוגר הזזה עם משוב לינארי

Hashing Terms

Hash Function	פונקצית תמצות (ערבול זה scrambling)
One Way Function	פונקציה חד-כוונית
One Way Hash Function	פונקצית תמצות חד-כוונית
Hash Value	תמצית
Message Authentication Code	קוד אמות הודעות
Birthday Paradox	פרדוקס יום ההלדת
Birthday Attack	התקפת יום הלדת
Collision	התנגשות
Collision Free Hash Function	פונקצית תמצות ללא התנגשויות
Compression Function	פונקצית 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	זהוי
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	לוגריתם 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 — שתוף סוד, (חלוקת סוד)

Threshold Scheme — סכמת סף

Share — שתף [SHETEF], (חלק)

Share Holder — שותף

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