1)

Asymmetric encryption

LECTURE 5

הצפנה א-סימטרית

2)

קריפטוגרפיה - סקירה

Cryptography - Review

-> Encryption or Cryptology – the name means secret writing – is probably the strongest defense in the arsenal of computer security protection.

-> Cryptography conceals data against unauthorized access.

-> הצפנה או קריפטולוגיה - פירוש השם הוא כתיבה סודית - היא ככל הנראה ההגנה החזקה בארסנל ההגנה של אבטחת המחשב

-> קריפטוגרפיה מסתירה נתונים מפני גישה לא מורשים.

3)

מפתחות הצפנה

Encryption Keys

A cryptosystem involves a set of rules of how to encrypt the plaintext and decrypt the ciphertext. The encryption and decryption rules, called **algorithms**, often use a device called a **key**, denoted by **K**, so that the resulting ciphertext depends on the original plaintext message, the algorithm, and the key value.

We write this dependence as **C = E(K, P)**. Essentially, **E** is a *set* of encryption algorithms, and the key **K** selects one specific algorithm from the set.

מערכת הקריפטו כוללת מערכת כללים כיצד להצפין את הפשוט-טקסט ולפענח את הצופן, כללי ההצפנה והפענוח, הנקראים אלגוריתמים, משתמשים לרוב במכשיר שנקרא מפתח, המסומן על-ידי K, כך שהצופן תלוי בהודעת הפשוט-טקסט המקורית, האלגוריתם וערך המפתח.

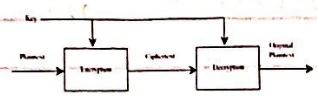
אנו כותבים תלות זו כ- $C=E(K,P)$. בעיקרו של דבר, E היא קבוצה של אלגוריתמי הצפנה, והמפתח K בוחר אלגוריתם ספציפי אחד מהסט.

4)

Encryption Keys

Symmetric (single-key or secret) key encryption:

the encryption and decryption keys are the same: P = D (K, E(K, P))



מפתחות הצפנה

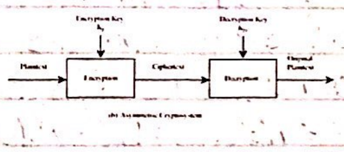
← הצפנה מפתחות סימטרית (יחיד או סודי):
מפתחים ההצפנה והפענוח זהים.

5)

Encryption Keys

Asymmetric (or public) key encryption:

Encryption and Decryption keys come in pairs. A decryption key, K_D, inverts the encryption of key K_E, so that P = D(K_D, E(K_E, P)).

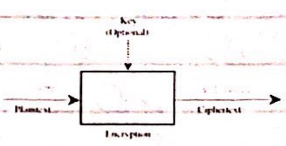


מפתחות הצפנה

← הצפנה מפתח אסימטרית (או ציבורית):
מפתחות הצפנה ופענוח מגיעים בזוגות, מפתח פענוח, K-D, ממיר את קידוד המפתח K_E, כך
P=D(K-D, E(K-E, P))

6)

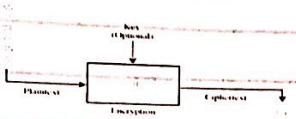
Stream Enciphering



הצפנת זרם

7)

Block Cipher



בלוק מוצפן

8)

מהי הצפנה סימטרית: DES

DES: The Data Encryption Standard

DES is a careful and complex combination of two fundamental building blocks of encryption: substitution and transposition.

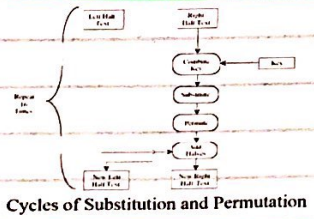
The algorithm derives its strength from repeated application of these two techniques, one on top of the other, for a total of 16 cycles.

DES encrypts 64-bit blocks by using a 56-bit key.

DES הוא שילוב מורכב ומדוקדק של שני אבני בניין בסיסיות של הצפנה: החלפה וטרנספוזיציה. האלגוריתם שואב את כוחו מיישום חוזר של שני טכניקות אלה, זו על גבי זו, בסך הכל על 16 מחזורים. DES מצפין מחסומים של 64 סיביות באמצעות מפתח 56 סיביות.

9)

DES: The Data Encryption Standard



Cycles of Substitution and Permutation

מהי הצפנה סימטרית
DES

מחלקה: החלפה ופרמוטציה
בדרגות שונות של מורכבות

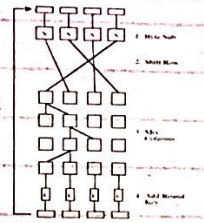
10)

DES: The Data Encryption Standard

Encrypts with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Encrypts with first key; then encrypt result with second key	Two 56-bit key	One doubles strength of 56-bit key version
Encrypts with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit key	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Encrypts with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit key	Gives strength equivalent to about 112-bit key about 72 quintillion ($72 * 10^{15}$) times as strong as 56-bit version

11)

AES: Advanced Encryption System



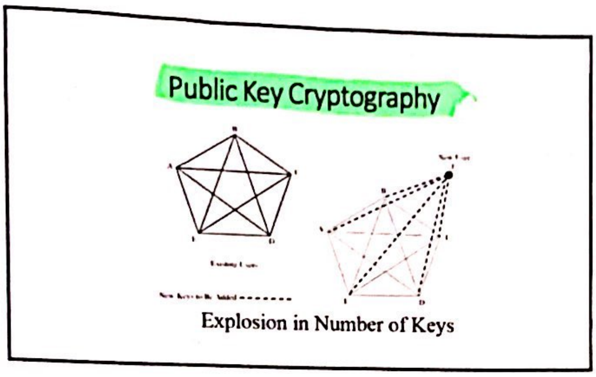
AES

12)

Comparison of DES and AES

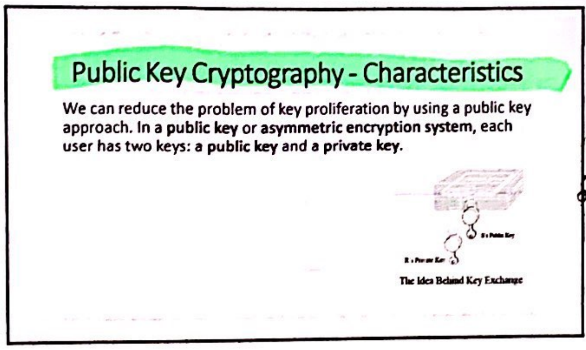
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticism invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

13)



קריפטוגרפיה של מפתח ציבורי

14)



קריפטוגרפיה של מפתח ציבורי - מאפיינים:

אנו יכולים לצמצם את בעיית התפשטות המפתח באמצעות גישת מפתח ציבורי במפתח ציבורי או במערכת הצפנה א-סימטרית, לכל משתמש שני מפתחות: מפתח ציבורי ומפתח פרטי

15)