THE UNIVERSITY OF ILLINOIS AT CHICAGO

UIC

CS 468: Network Security

Lecture 3: Intro to Cryptography

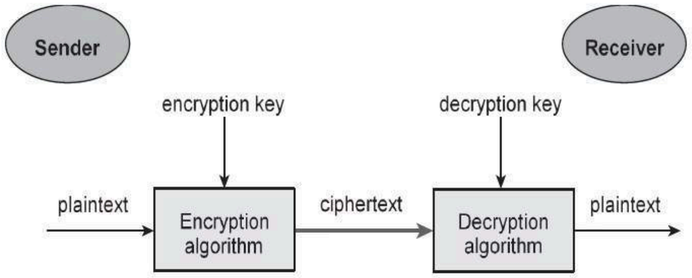
Jason Polakis
polakis@uic.edu

Tuesday, 09/03/2024

https://www.cs.uic.edu/~polakis/

Cryptographic Algorithms

- Algorithms used mainly for two purposes
  - Encryption/Decryption: transformation of plaintext to ciphertext / vice versa
  - Signature: Computation of message value and verification



- Encryption categories
  - Symmetric (same key used for encryption and decryption)
    - DES, 3DES, AES, RC2, RC5, RC4, Blowfish,..
  - Asymmetric (one key for encryption, one key for decryption)
    - RSA, DSA,…

- Encryption ciphers
  - Stream cipher (every bit is encrypted separately)
  - Block cipher (encryption is performed on blocks of bits)

Encryption Techniques / Building Blocks

- **Substitution**: every letter of the plaintext is substituted with another letter
  - Substitution usually applies *confusion* (make it difficult to determine how message and key were transformed into cipher)

- **Transposition**: the positions held by characters are shifted according to a regular system
  - Transposition's goal is usually *diffusion*: spread changes across ciphertext

Encryption Techniques (substitution)

- Substitution
  - Every letter of the plaintext is substituted with another letter
  - E.g., we may build the following table:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z (plaintext)
f g h i j k l m n o p q r s t u v w x y z a b c d e (encryption)
```

  - `Plaintext:  i have often seen a cat without a grin`
  - `Ciphertext: n mfaj tkyjs xjjs f hfy bnymtzy f lwns`
  - Better: `nmfajtkyjsxjjsfhfybnymtzyflwns`
  - Break with: ***frequency analysis*** and distribution
    - Some letters are more common than others
    - This can differ across languages (e.g., “e” most common in English)
    - Some bigrams and trigrams in English are more common than others
    - en, re, er, nt, th, ent, ing, ion, and
    - Frequency distribution tables available

Encryption Techniques (substitution)

- Desirable: flatter frequency distribution in ciphertext
  - E.g., one encryption alphabet for odd positions in plaintext and one for even positions in plaintext

a b c d e f g h i j k l m n o p q r s t u v w x y z (plaintext, odd)

f g h i j k l m n o p q r s t u v w x y z a b c d e (encryption)

a b c d e f g h i j k l m n o p q r s t u v w x y z (plaintext, even)

n s x c h m r w b g l q v a f k p u z e j o t y d i (encryption)

i have often seen a cat without a grin

n wfyj fkeja xhja f xfe bbywtjy n luna

- Alternatively, you can assign more substitution characters to high frequency letters (e.g., “e” maps to 3 characters, “q” maps to 1)

Encryption Techniques (substitution)

- Polyalphabetic substitutions
  - Different encryption alphabets used in cycle
- Flatter frequency distribution but still not strong

One-time Pad

- Ideal: infinite non-repeating sequence of alphabets
- One time pads
  - Random text with length equal to that of the message is used for substitution
  - Problems: receiver must have it too (distribution, storage)

XOR plaintext with a keystream

1882 Frank Miller [Bellovin '11]

1917 Vernam/Mauborgne cipher

Information-theoretically secure against ciphertext-only attacks (Shannon 1949)

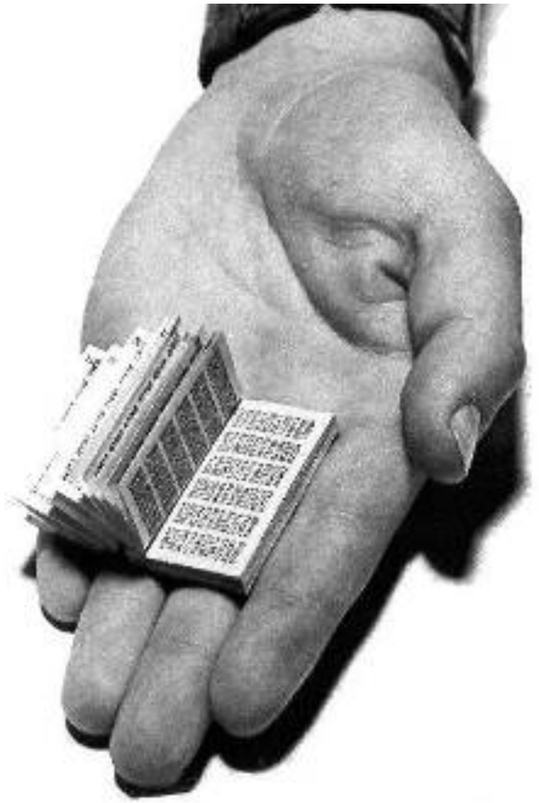
The keystream must be

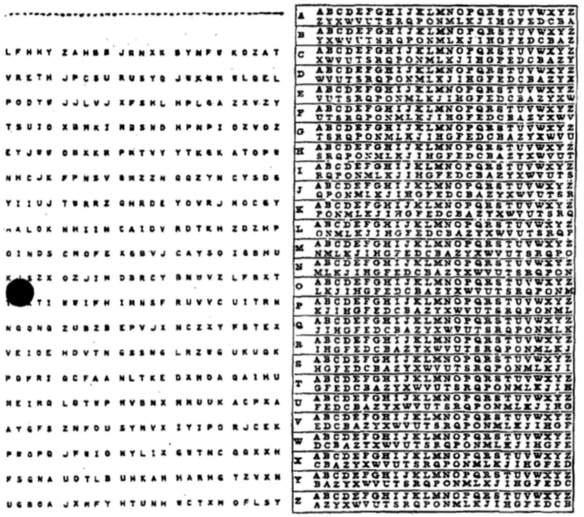
Truly random

As long as the plaintext

Kept completely secret

Used only once…





One-time Pad

Plaintext space: *all n-bit sequences*

Ciphertext space: *all n-bit sequences*

Key space: *all n-bit sequences*

Encryption algorithm: $E(p, k) = p \oplus k$ *(bit by bit)*

Decryption algorithm: $D(c, k) = c \oplus k$ *(bit by bit)*

Advantages

Easy to compute: simple XOR operation

Impossible to break: information-theoretically secure

Disadvantages

Key size: must be as long as the plaintext

Key distribution: how can the sender provide the key to the receiver securely?

Encryption Techniques (Transpositions)

- Transposition
  - The message's letters remain the same. Their order is rearranged
- Simple e.g., columnar transpositions
  - "i have often seen a cat without a grin"
  - ihave iosct
    often ahfea
    seena hgate
    catwi torve
    thout nwuie
    agrin naitn

Cryptanalysis of Columnar Transpositions

- Anagramming—sliding pieces of ciphertext around, then looking for sections that look like anagrams of words in source language and solving the anagrams. Once such anagrams have been found, they reveal information about the transposition pattern, and can consequently be extended.

-

Stream Ciphers

- The substitution examples we saw are stream ciphers
  - Every symbol of plaintext is immediately converted in ciphertext
  - Transformation depends only on symbol, key, and logic of algorithm (XOR for example)
- Advantages:
  - Fast, encryption is immediate
  - Low error propagation, an error affects only one character
- Disadvantages:
  - Low diffusion: each symbol separately enciphered. All info on that symbol contained in one symbol of ciphertext. Frequency distribution, bigram analysis, Kasiski method possible
  - Susceptible to malicious insertions and modifications (an attacker that breaks the algorithm can introduce fake text that appears authentic)

Block Ciphers

- Columnar transpositions are block ciphers
  - We need to have chunk of message available, cannot encrypt one symbol at a time
- Encrypt a group of plaintext as a *block*
- Advantages:
  - Diffusion: one ciphertext block depends on several plaintext letters
  - Immunity to insertions: blocks of symbols are enciphered, insertion would change the length of the block, decryption would be incorrect.
- Disadvantages:
  - Slower than stream, must wait for entire block to become available
  - Error propagation, an error may affect the transformation of all characters in a block (e.g., if a letter is dropped in columnar transposition).

Computational Difficulty/Strength

Modern cryptography: seek guarantees about the "strength" of encryption schemes

- Codes, secret writing, and other older encryption schemes were ad hoc and eventually broken

Information-theoretic security

- Cannot be broken even with unlimited computing power: *there is simply not enough information*
- Not possible if the key is shorter than the message size → impractical

Computational security

- Can be broken with enough computation, but *not in a reasonable amount of time (or time required exceeds the useful lifetime of the information)*
- Rely on *computationally hard* problems: easy to compute but hard to invert (integer factorization, discrete logarithm, …)
- Assume *computationally limited adversaries* → frustrate exhaustive enumeration

Symmetric Encryption Systems

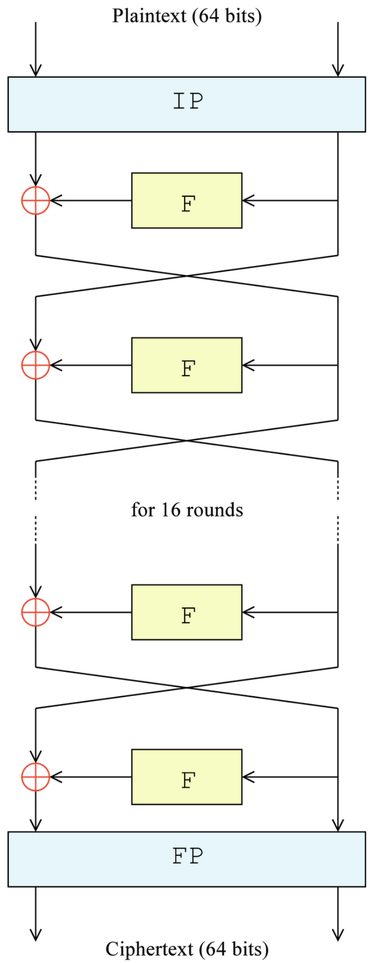
- Same key is used to encrypt and decrypt
- Key must be kept secret
- If stolen, attacker may decrypt or change the messages
- Distribution of keys may be a problem
  - By hand
  - In pieces over different channels

The (In)Famous Data Encryption Standard (DES)

- Symmetric key system
- Data is divided into blocks of 64 bits
- Encryption performed on blocks of 64 bits with key of 64 bits
  - Actual key length is 56 bits (drops every 8th bit which is only used for parity), used to generate 16 different 48-bit subkeys
- Based on substitutions and permutations

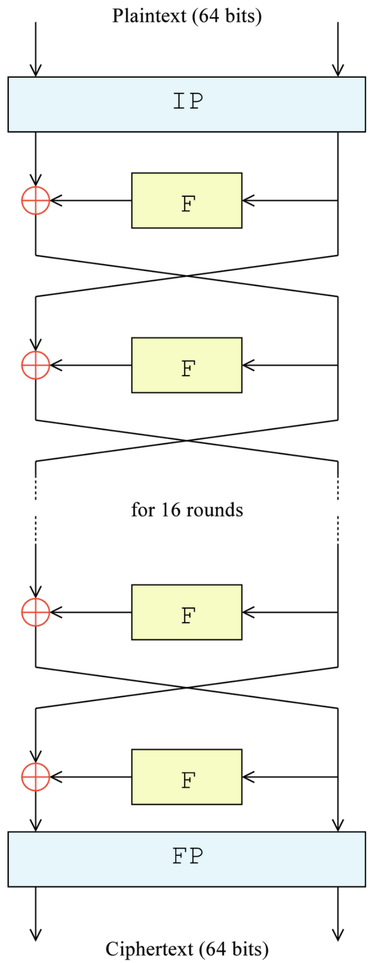
DES rounds (source: wikipedia)

- ⊕ symbol denotes the exclusive-OR (XOR) operation
- Each block goes through an initial permutation IP (based on a table)
- 64-bit data blocks are divided into two halves (32 bits each)
  - the F-function operates on a 32-bit half
- The process consists of 16 identical main rounds, each using one subkey
- Each block goes through a final permutation FP that is the inverse of IP

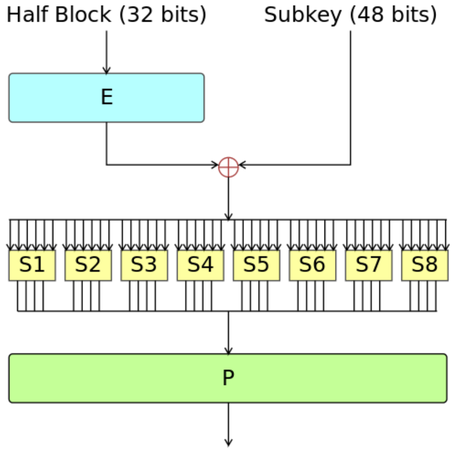


DES round

- The results of F-function (32 bits) are XORed with the left half
- Next, the original right half becomes the left half and the XOR's result becomes the right half for the next round (criss-crossing)
- Decryption applies the same steps in reverse



F-function



- The half is expanded (E) to 48 bits by duplicating half of the bits and XOR-ed with a subkey
- The block goes into S-Box (substitution box)
  - Transforms the 48 bits back into 32 bits
- The 32 bits from the S-Box go into a P-Box (permutation box), which moves them around according to a table

Differential Cryptanalysis

- Technique that can be used for all substitution and permutation algorithms
- Select two plaintexts with subtle differences and study the effects on ciphertexts
- This may allow to recover portions of the key
- For DES, three attacks have been proposed - considered theoretical and infeasible to deploy in practice

DES analysis

- Heavily scrutinized by cryptographers/cryptanalysts
- Controversial
  - Why did NSA choose specific values in the S-Boxes and in the P-Boxes? There are many possibilities? Were there any trapdoors?
  - Key length is too short. There are 2^56 possible keys
  - Brute force attacks have been able to find the key in a short amount of time
    - EFF DES Cracker (parallel customized chips, $250K in 1998): tested 90 billion keys per second. Took 56 hours to decrypt

Problems with DES

- DES is not recommended for use anymore
- New standard called AES chosen as replacement in 2001
- However, DES was still being used a few years ago (e.g., MSCHAPV2)

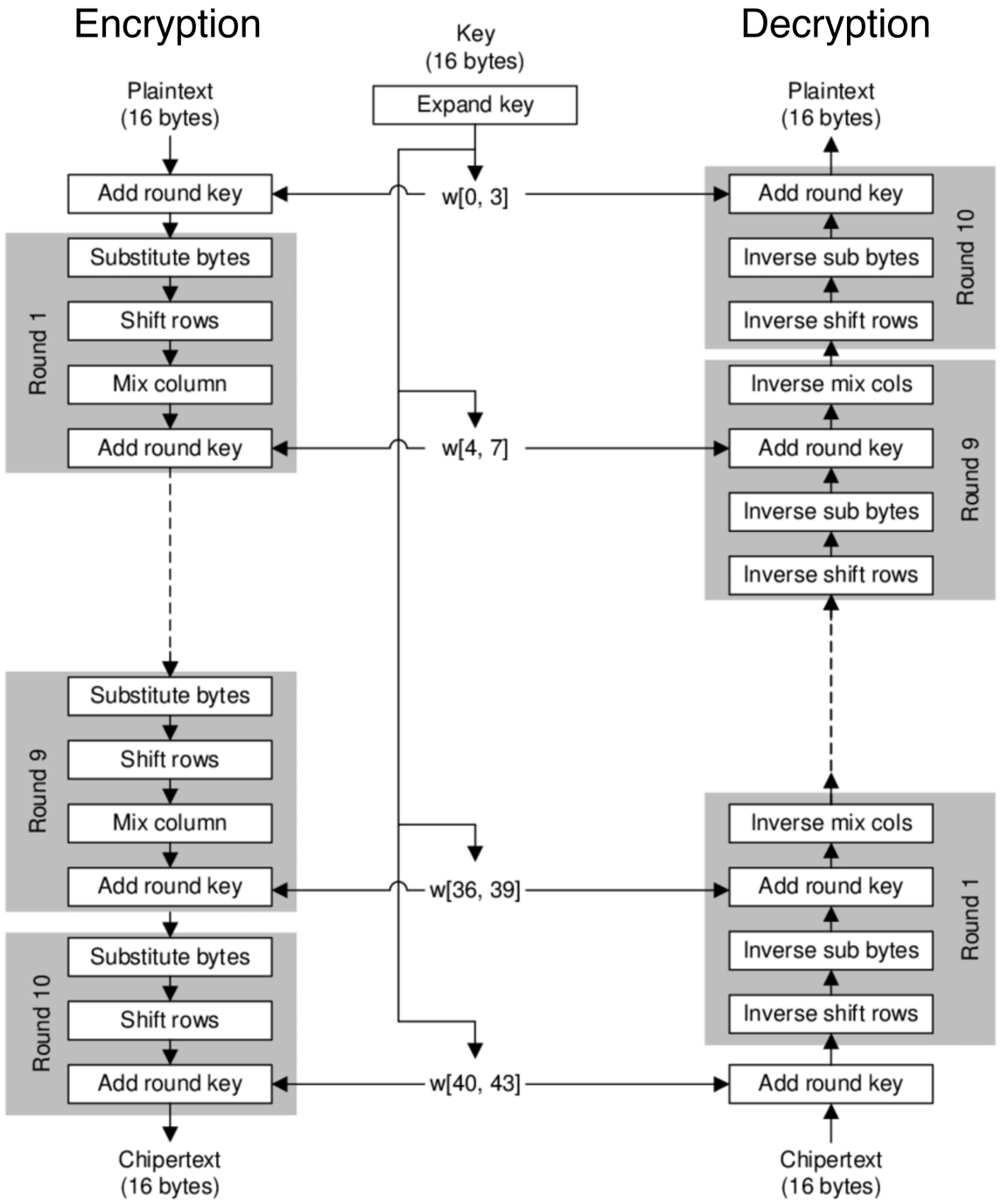
3DES

- Standardized in 1999
- uses 3 keys and 3 executions of the DES algorithm
  - has an effective key size of 168
- $C = E(K_3, D(K_2, E(K_1, P)))$
- $P = D(K_1, E(K_2, D(K_3, C)))$

- Advantages
  - larger key size offers more security
  - underlying DES algorithm has been heavily scrutinized
- Disadvantage
  - sluggish to run in software
  - uses small (64 bit) block size

AES

- Successor to DES
- Key length of 128 bits and 10 rounds
  - key expanded into array of forty-four 32-bit words, 4 words used per round
- 4 stages of changes per round
  - S-boxes based on algebraic finite field theory (provides the non-linearity in the cipher)
  - Shift rows (per-row permutation, cyclically shifts the bytes in each row by a certain offset)
  - Mix columns: alters each byte in a column as a function of all the bytes in the column, provides diffusion
  - Add round key: XOR current block with the subkey
- Direct attacks against AES so far have proven unsuccessful



Only 3 transformations in final round

Only 3 transformations in final round

Questions?