

# CS 4803

## Computer and Network Security

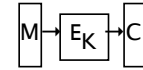
Alexandra (Sasha) Boldyreva

### Block ciphers. Pseudorandom functions.

1

### Block ciphers

Building blocks for symmetric cryptography.



Examples: DES, 3DES, AES...

- A block cipher  $E$  is a collection of functions from  $n$  bits to  $n$  bits. Each function is fully specified by a  $k$ -bit key.
- Notation: for every  $K \in \{0,1\}^k$ ,  $M \in \{0,1\}^n$   $E_K(M)$  is  $n$ -bit output
- For every  $K \in \{0,1\}^k$ ,  $E_K(\cdot)$  is a permutation (one-to-one and onto function). For every  $C \in \{0,1\}^n$  there is a single  $M \in \{0,1\}^n$  s.t.  $C = E_K(M)$
- Thus each block cipher has an inverse for every key:  $E_K^{-1}(\cdot)$  s.t.  $E_K(E_K^{-1}(C)) = C$ ,  $E_K^{-1}(E_K(M)) = M$  for all  $M, C \in \{0,1\}^n$
- For every  $K \in \{0,1\}^k$ ,  $E_K(\cdot), E_K^{-1}(\cdot) : \{0,1\}^n \rightarrow \{0,1\}^n$

2

### DES

- Key length  $k=56$ , input and output length  $n=64$
- 1973. NBS (National Bureau of Standards) announced a search for a data protection algorithm to be standardized
- 1974. IBM submits a design based on "Lucifer" algorithm
- 1975. The proposed DES is published
- 1976. DES approved as a federal standard
- DES is highly efficient:  $\approx 2.5 \cdot 10^7$  DES computations per second

3

### Security of block ciphers

- Any block cipher  $E$  is subject to exhaustive key-search: given  $(M_1, C_1 = E(K, M_1)), \dots, (M_q, C_q = E(K, M_q))$  an adversary can recover  $K$  (or another key consistent with the given pairs) as follows:

$EKS_E((M_1, C_1), \dots, (M_q, C_q))$

For  $i=1, \dots, 2^k$  do

if  $E(T_i, M_1) = C_1$  then //  $T_i$  is  $i$ -th  $k$ -bit string //

if  $E(T_i, M_j) = C_j$  for all  $2 \leq j \leq q$  then return  $T_i$  EndIf

EndIf

EndFor

4

## Security of block ciphers

- Exhaustive key search takes  $2^k$  block cipher computations in the worst case.
- On the average  $2^{k-1}$
- DES has a property that  $DES_K(x) = \overline{DES_{\overline{K}}(\overline{x})}$ , this speeds up exhaustive search by a factor of 2
- For DES ( $k=56$ ) exhaustive search takes  $2^{55}/2.2.5 \cdot 10^7$  that is about 23 years

5

## Security of DES

- There are more sophisticated attacks known:
  - differential cryptanalysis: finds the key given about  $2^{47}$  chosen plaintexts and the corresponding ciphertexts
  - linear cryptanalysis: finds the key given about  $2^{42}$  known plaintext and ciphertext pairs
- These attacks require too many data, hence exhaustive key search is the best known attack. And it can be mounted in parallel!
- A machine for DES exhaustive key search was built for \$250,000. It finds the key in about 56 hours on average.
- A new block cipher was needed....
- Triple-DES:  $3DES(K1||K2,M)=DES(K2, DES^{-1}(K1, DES(K2,M)))$ .
  - 3DES's keys are 112-bit long. Good, but needs 3 DES computations

6

## Advanced Encryption Standard (AES)

- 1998. NIST announced a search for a new block cipher.
- 15 algorithms from different countries were submitted
- 2001. NIST announces the winner: an algorithm Rijndael, designed by Joan Daemen and Vincent Rijmen from Belgium.
- AES: block length  $n=128$ , key length  $k$  is variable: 128, 192 or 256 bits.
- Exhaustive key search is believed infeasible

7

## Limitations of key-recovery based security

- A classical approach to block cipher security: key recovery should be infeasible.
- I.e. given  $(M1,E(K,M1),\dots,Mq,E(K,Mq))$ , where  $K$  is chosen at random and  $M1,\dots,Mq$  are chosen at random (or by an adversary), the adversary cannot compute  $K$  in time  $t$  with probability  $\epsilon$ .
- Necessary, but is it sufficient?
- Consider  $E'(K,M1||M2)=E(K,M1)||M2$  for some "good"  $E$ . Key recovery is hard for  $E'$  as well, but it does not look secure.
- Q. What property of a block cipher as a building block would ensure various security properties of different constructions?

8

## Intuition

- We want that (informally)
  - key search is hard
  - a block cipher output does not leak the input
  - a block cipher output does not leak bits of the input
  - a block cipher output does not leak any function of the input
  - ....
  - there is a "master" property of a block cipher as a building block that enables security analysis of protocols based on block ciphers
- It is good if the block cipher outputs "look" random

9

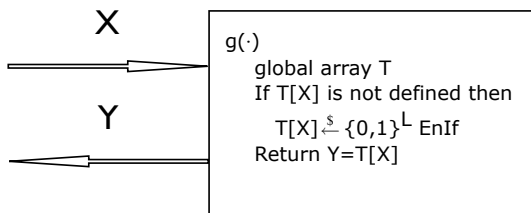
- Pseudorandom functions (PRFs) is a very important notion in cryptography.
- A good block cipher should be a pseudorandom function, i.e. (informally) its instances behave like a random function, and thus no information can be learned from its behavior.
- What is a random function (our ideal object)?
  - It is a function chosen at random from the set of ALL possible functions from  $n$  bits to  $n$  bits.
  - We are interested in the input-output behavior of a random function. Let's imagine that we have access to a subroutine that implements such a function:

```
g( $X \in \{0,1\}^n$ )
global array T
If T[X] is not defined then
  T[X]  $\xleftarrow{\$}$   $\{0,1\}^n$  EndIf //pick a random n-bit string
Return T[X]
```

10

## "Black box" access

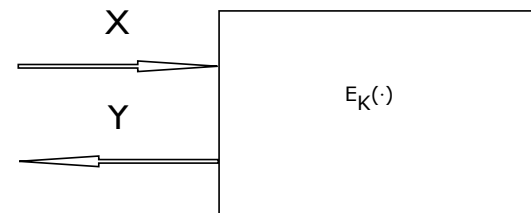
Imagine a computer has an executable program for a random function and you can use it via an input-output interface



11

## "Black box" access

Imagine the computer also has an executable program for a block cipher  $E$  specified by a random key  $K$ , and you can use the program via an input-output interface



12

## Pseudorandom functions (PRFs)

- Informally, a block cipher is a PRF if the input-output behavior of its random instance is computationally indistinguishable from that of a random function.
- Meaning if you have a black-box access to a computer with either a random function or a block cipher instance inside, you cannot efficiently tell which.

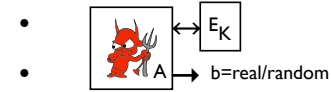
13

## PRFs (more formally)

- Def. Fix a block cipher  $E$

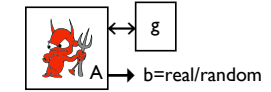
- Experiment  $\text{prf-real}(E, A)$

- pick a  $k$ -bit key  $K$  at random



- Experiment  $\text{prf-random}(E, A)$

pick a function at random from all functions mapping  $n$  bits to  $n$  bits



$E$  is a secure PRF if any adversary with "reasonable" resources outputs the same guess (i.e. "real") in both experiments with "almost" equal probability.

The difference between these probabilities of outputting "real" in two experiments is called  $\text{prf-advantage}$  of  $A$  in attacking  $E$ . I.e.

$E$  is a secure PRF if  $\text{prf-advantage}$  of any adversary with "reasonable" resources is "close" to 0.

14

## Resources of an adversary

- The running time.
- The number of queries  $A$  makes.
- The total length of all queries.

15

## Security of block ciphers

- Conjectures:
  - DES and AES are PRFs.

16