

# Block Ciphers

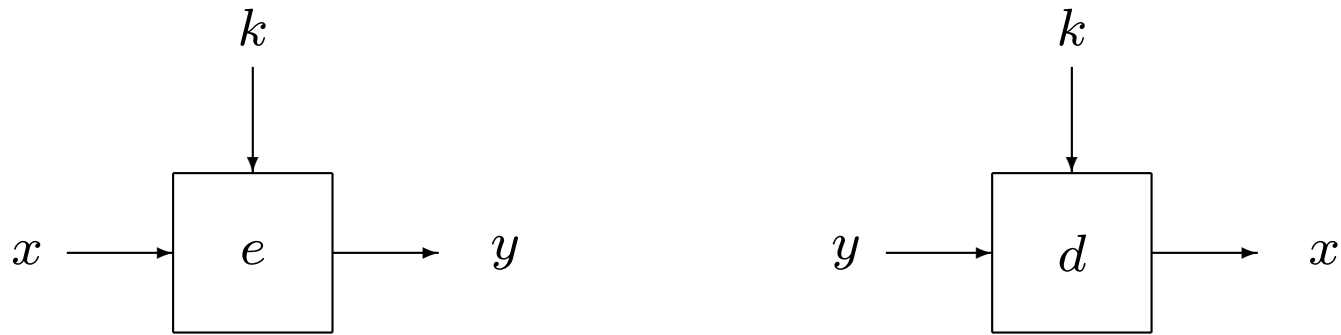
Alex Biryukov, K.U. Leuven

Lars R. Knudsen, Technical University of Denmark

November 26, 2002

## Block ciphers

$$e : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^n \quad d : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^n$$



- permutation:  $d_k(e_k(x)) = x \quad \forall x$
- given  $x$  and  $k$  easy to compute  $y$   
given  $y$  and  $k$  easy to compute  $x$
- one-way function:  $f(k) = e_k(x_0)$  for fixed  $x_0$

## Block ciphers

- family of  $2^\ell$  permutations of  $n$  bits
- one  $\ell$ -bit key
  - specifies one permutation,  $e_k(\cdot)$
  - yields an algorithm which takes  $x$  to  $y = e_k(x)$  and  $y$  to  $d_k(y)$
- #  $n$ -bit permutations:  $2^n! \simeq (2^{n-1})2^n$
- #  $n$ -bit permutations in block cipher:  $2^\ell$   
(AES:  $n = \ell = 128$ )
- design principle: choose the  $2^\ell$  permutations uniformly at random from the set of all  $2^n!$  permutations

## Block ciphers - applications

- encryption
- used as building block in
  - hash algorithms
  - MAC algorithms
  - stream cipher systems

## Shannon's theory

Perfect secrecy (  $\Pr(x|y) = \Pr(x)$  ) obtained  
**if and only if** key used only once **and**  $\ell \geq n$

**Unicity distance:** How many inputs/outputs needed to be able **at least in theory** to uniquely determine secret key?

$$\min_m : H(k | x_1, \dots, x_m, y_1, \dots, y_m) \approx 0, \quad m = \ell/n$$

$m$  is (very) small for all popular block ciphers

## Shannon's thoughts

How can we ever be sure that a system, which is not perfect will require a large amount of work to break with *every* method of analysis

1. Make it reducible to some known difficult problem.

Examples:

(a) Solve a large system of nonlinear equations

(b) Factoring

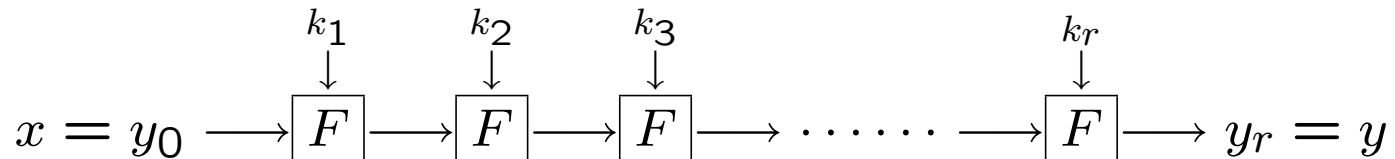
(c) Discrete log

Minimum: make it secure against all known attacks

## Shannon's principles - confusion, diffusion

- $x = x_1, \dots, x_n, \quad k = k_1, \dots, k_\ell, \quad y = y_1, \dots, y_n,$
- $\forall i : y_i = f_i(x_1, \dots, x_n, k_1, \dots, k_\ell)$
- confusion:  $f_i$  non-linear and complex!
- diffusion:  $y_i$  depends on all/many of inputs to  $f_i$
- confusion obtained by substitutions
- diffusion obtained by (bit) permutations
- product = (substitution  $\times$  permutation) <sup>$i$</sup>

## Iterated (product) ciphers



- $x = y_0$  plaintext
- $y_i = F(k_i, y_{i-1})$ ,       $F$  round function
- $y_r$  ciphertext
- round keys  $k_1, k_2, \dots, k_r$
- $F$  invertible for fixed key, weak by itself
- Ex. Feistel ciphers

## Attacks on iterated ciphers

- can (in principle) be applied to any number of rounds
- two types
  - success decreases exponentially with number of rounds  
Ex.: *differential cryptanalysis, linear cryptanalysis*
  - success independent of no. of rounds or decreases but not exponentially with number of rounds  
Ex.: *related keys, slide attacks, algebraic attacks*

## Algebraic attacks

$f(x) = x^{2^k+1}$  and  $f(x) = x^{-1}$  in  $\text{GF}(2^n)$  good properties against differential and linear attacks

Consider function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ ,  $f(x) = y$

**Definition** I/O-degree is smallest algebraic degree of multivariate expressions  $g(y_{m-1}, \dots, y_0, x_{n-1}, \dots, x_0) = 0$ , which holds with certainty

$f(x) = x^{2^k+1}$  and  $f(x) = x^{-1}$  have I/O-degree 2

Encryption systems based solely on low I/O degree functions are susceptible to *algebraic* attacks

## “Proofs” of security

- Perfect secrecy
- Luby-Rackoff (Feistel construction)
- Even-Mansour (randomly chosen permutation with key whitening)
- Constructions (provably) secure against (conventional) differential and linear attacks  
Ex. Kasumi
- Decorrelation theory

## Future research problems

- construct efficient secret-key block ciphers whose security reduces to a problem known to be difficult
- construct efficient secret-key block ciphers with a proof of security against all known attacks
- differential, linear, boomerang, multiset etc: how far can we get?
- explore algebraic attacks: relinearisation ? XSL?
- number of rounds in iterated ciphers?
- trapdoor block ciphers?  $\rightsquigarrow$  public-key systems