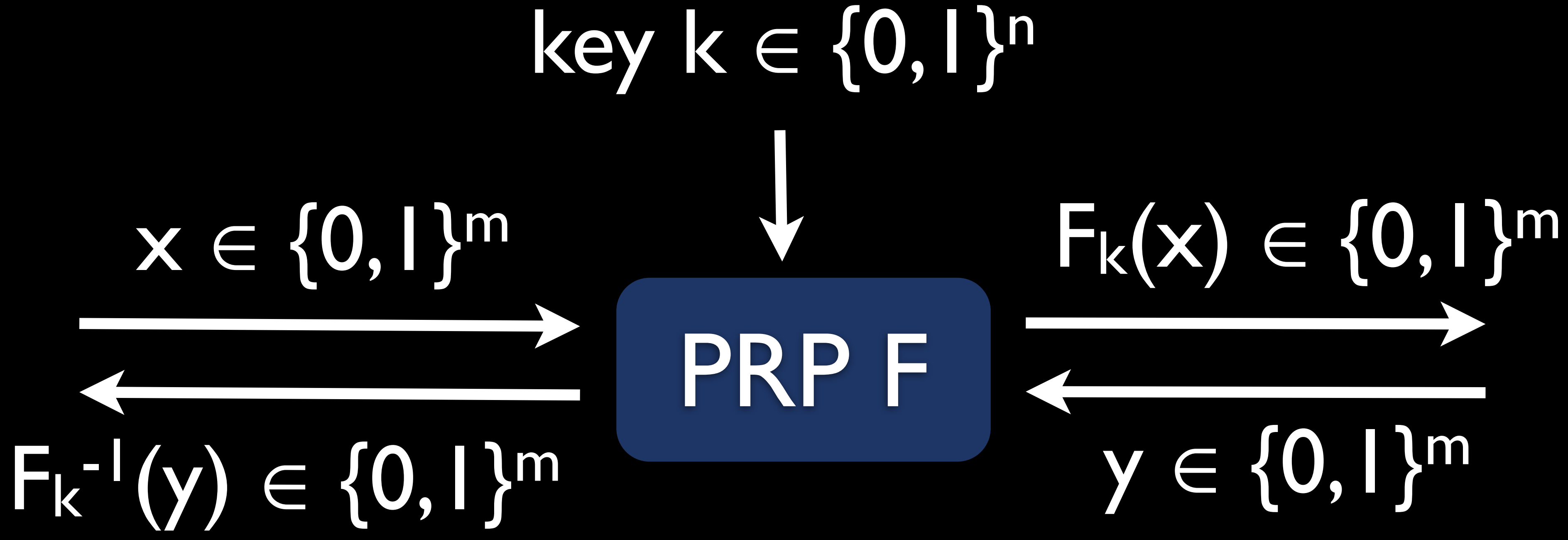
Introduction to Modern Cryptography

7th lecture:

Practical Block Ciphers: DES & AES

some of these slides are copied from or heavily inspired by the
University College London MSc InfoSec 2010 course given by Jens Groth
Thank you very much!

Strong Pseudorandom Permutations



key $k \in \{0,1\}^n$

$x \in \{0,1\}^m$

PRP F

$F_k(x) \in \{0,1\}^m$

$F_k^{-1}(y) \in \{0,1\}^m$

$y \in \{0,1\}^m$

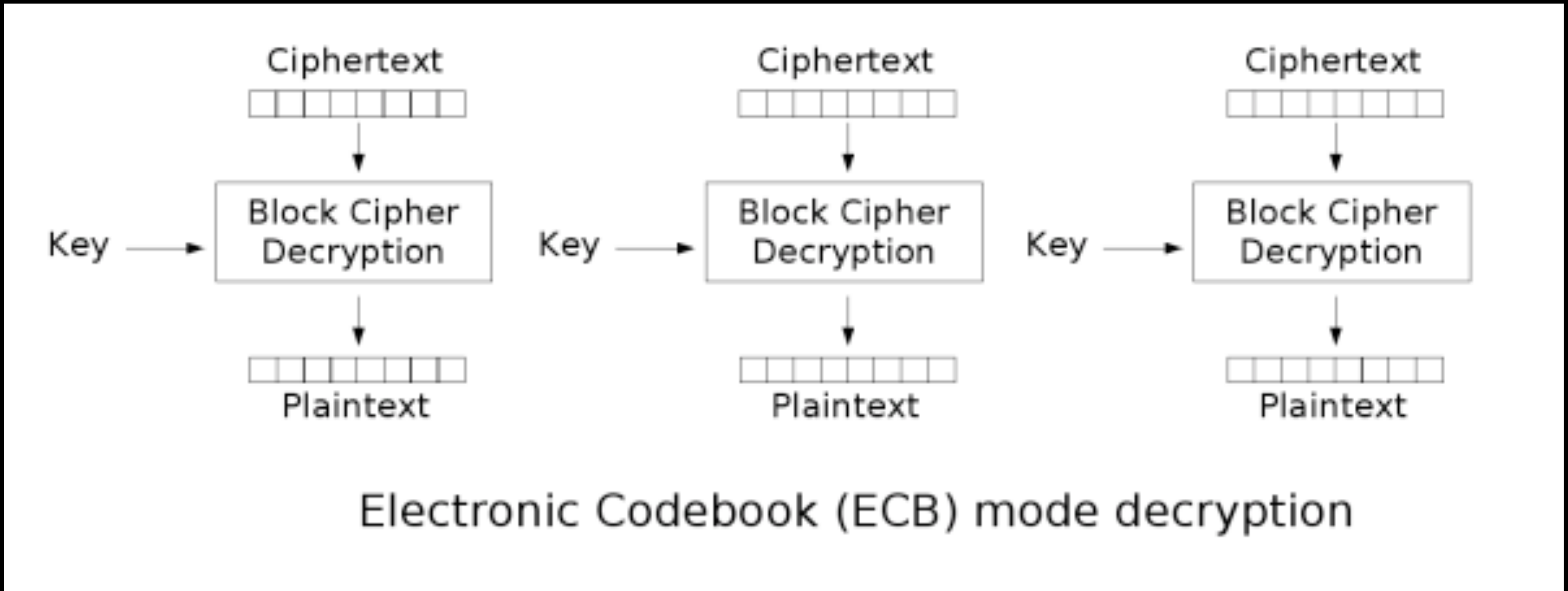
- F and F^{-1} bijective poly-time functions
- for every PPT distinguisher D:
  $| \Pr[D^{F_k(\,), F_k^{-1}(\,)}(1^n)=1] - \Pr[D^{f(\,), f^{-1}(\,)}(1^n) =1] | \leq \text{negl}(n)$
  where $k \leftarrow \{0,1\}^n$ and $f \leftarrow \text{Perm}_n$.

Possible Types of Attacks

- ciphertext-only: Adv gets $\{F_k(x_i)\}$ for some $\{x_i\}$ unknown to Adv
- known-plaintext: Adv gets pairs of in- and outputs $\{(x_i,F_k(x_i))\}$
- chosen-plaintext: Adv gets $\{(x_i,F_k(x_i))\}$ for $\{x_i\}$ of her choice
- chosen-ciphertext: Adv gets $\{(x_i,F_k(x_i))\}$ and $\{(F_k^{-1}(y_i),y_i)\}$ for $\{x_i\}$, $\{y_i\}$ of her choice
- Possible goals: key recovery or distinguishing from random permutation

WARNING

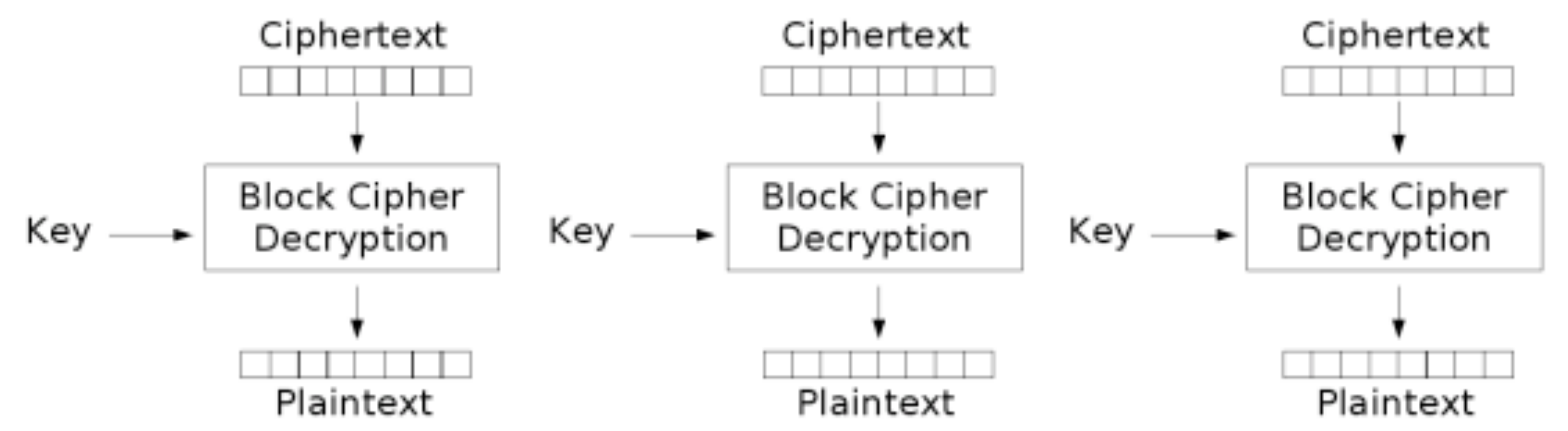
- block ciphers are NOT secure encryption schemes



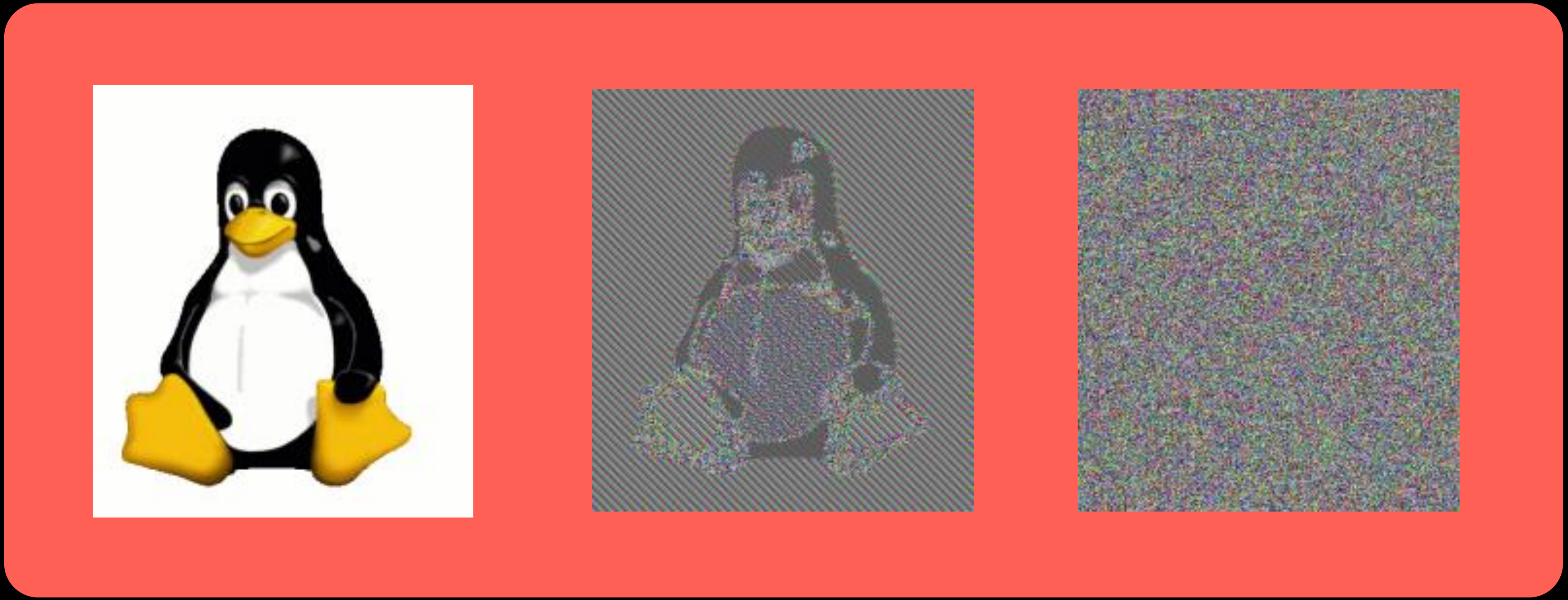
Electronic Codebook (ECB) mode decryption

WARNING

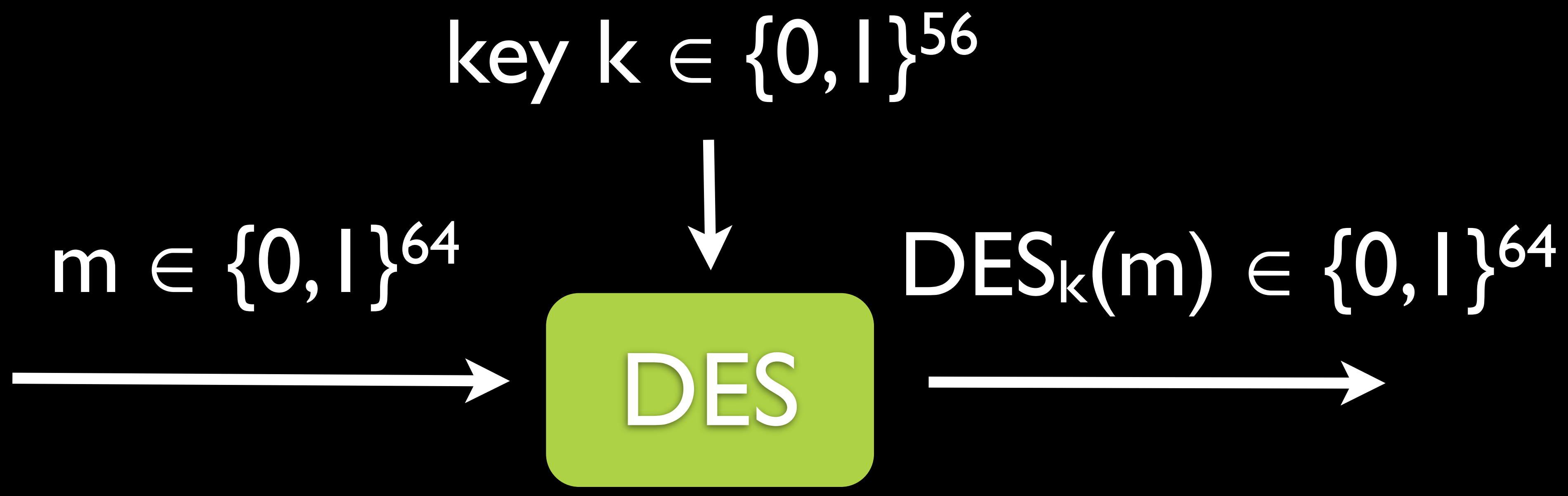
- block ciphers are NOT secure encryption schemes



Electronic Codebook (ECB) mode decryption



Data Encryption Standard (DES)



key $k \in \{0,1\}^{56}$

$m \in \{0,1\}^{64}$

DES

$\mathrm{DES}_k(m) \in \{0,1\}^{64}$

- developed by IBM in the 1970s
- National Security Agency (NSA) suggested last minute change
- became Federal Information Processing Standard (FIPS) in 1977
- widely used, even today

Horst Feistel

1915 - 1990

- MIT, Stanford
- @IBM: Feistel network

- moved to the US as 19 years old
- placed under house arrest during WWII
- then became American

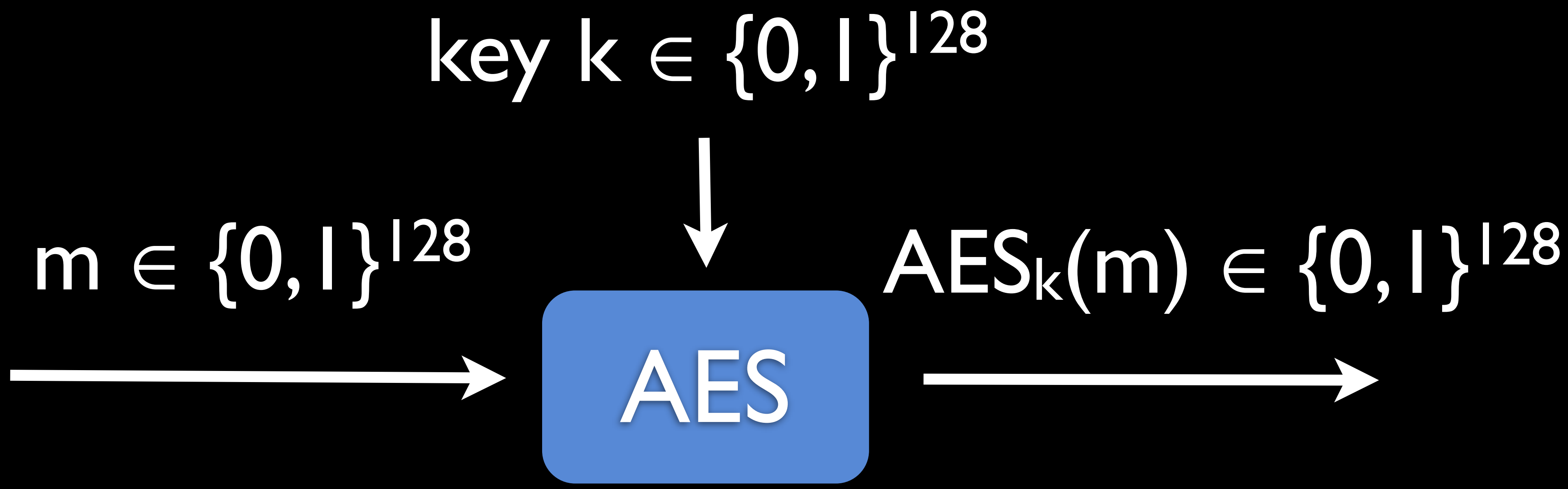
Brute Force Attacks

- 2^{56} possible keys, 2^{64} possible ciphertexts
- One known-plaintext pair $(x, DES_k(x))$ determines the key with probability $1 - 2^{56}/2^{64} > 99\%$ (assuming each key maps x to a random ciphertext)
-

year	project	time
1997	DESCHALL, internet	96 days
1998	distributed.net	41 days
1998	Deep Crack, 250 k $	2 days
2008	COPACOBANA, 10 k EUR	1 day

- DES has excellent design, but key is too short!

Advanced Encryption Standard (AES)



key $k \in \{0,1\}^{128}$

$m \in \{0,1\}^{128}$

AES

$\mathrm{AES}_k(m) \in \{0,1\}^{128}$

- 1997: NIST announces competition
  Criteria: efficiency, security, royalty-free
- winner out of 15 submissions: Rijndael
- faster than DES in both soft- and hardware
- currently no (close to) efficient attacks known

John Daemen
*1965

Vincent Rijmen
*1970

- Belgians
- KU Leuven

- 1997: Rijndael