CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Symmetric Key Encryption

Video Summary

- What is symmetric key encryption
- Assumptions
- Symmetric key encryption algorithms (DES, 3DES, AES)
- Attacks on Encryption Algorithms

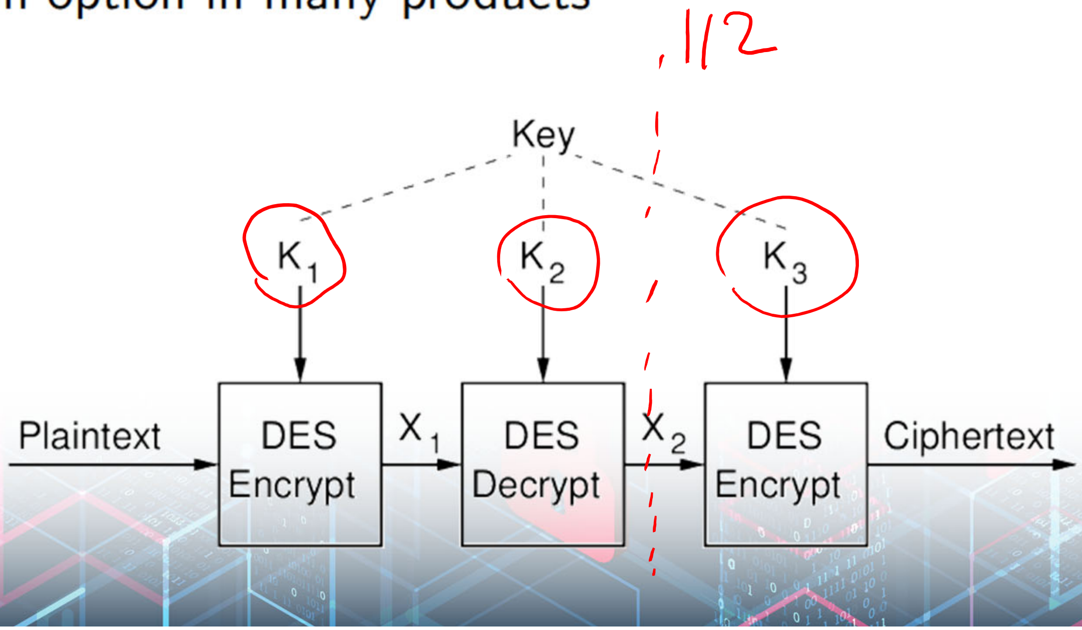
Data Encryption Standard (DES)

- Designed by IBM and NSA; standardised by NIST in 1977 as FIPS-46
  - 1999: NIST recommended Triple-DES; DES only for legacy systems
  - 2005: FIPS-46 standard withdrawn
- Block size: 64 bits
- Key length: 56 bits (64 bits, but 8 are parity)
- Initial and final permutations, then 16 rounds, each involving permutations and substitutions
- Decryption is almost identical to encryption → single implementation for both algorithms
- Key size is insecure; algorithm considered secure

Triple-DES (3DES)

56
56
56

- Standardised by ANSI/NIST in 1998/99
- Applies DES three times: Encrypt, Decrypt, Encrypt
- Block size: 64 bits
- Key length: 168 bits (options for 112 and 56 bits)
- Three times slower than DES
- Status: banks still use in many applications; available as an option in many products



Advanced Encryption Standard (AES)

- NIST held competition to select algorithm to replace DES/3DES in 1997
  - Won by Rijndael algorithm by Rijmen and Daemen
  - 2001: Standardised as FIPS-197
- Block size: 128
- Key length: 128, 192, 256 bits
- Substitution-permutation network
- Status: used in many products, e.g. WiFi (WPA), full disk encryption (BitLocker, FileVault2, dm-crypt, LUKS), Internet security (HTTPS), . . .

2^{128}

2^{192}

2^{256}

Other Symmetric Encryption Algorithms

- Blowfish (Schneier, 1993): 64 bit blocks/32–448 bit keys; Feistel structure $\rightarrow 2^{448}$
- Twofish (Schneier et al, 1998): 128/128, 192, 256; Feistel structure
- Serpent (Anderson et al, 1998): 128/128, 192, 256; Substitution-permutation network
- Camellia (Mitsubishi/NTT, 2000): 128/128, 192, 256; Feistel structure
- IDEA (Lai and Massey, 1991): 64/128
- CAST-128 (Adams and Tavares, 1996): 64/40–128; Feistel structure
- CAST-256 (Adams and Tavares, 1998): 128/up to 256; Feistel structure
- RC5 (Rivest, 1994): 32, 64 or 128/up to 2040; 2^{2040} Feistel-like structure

Attacks on Symmetric Key Encryption

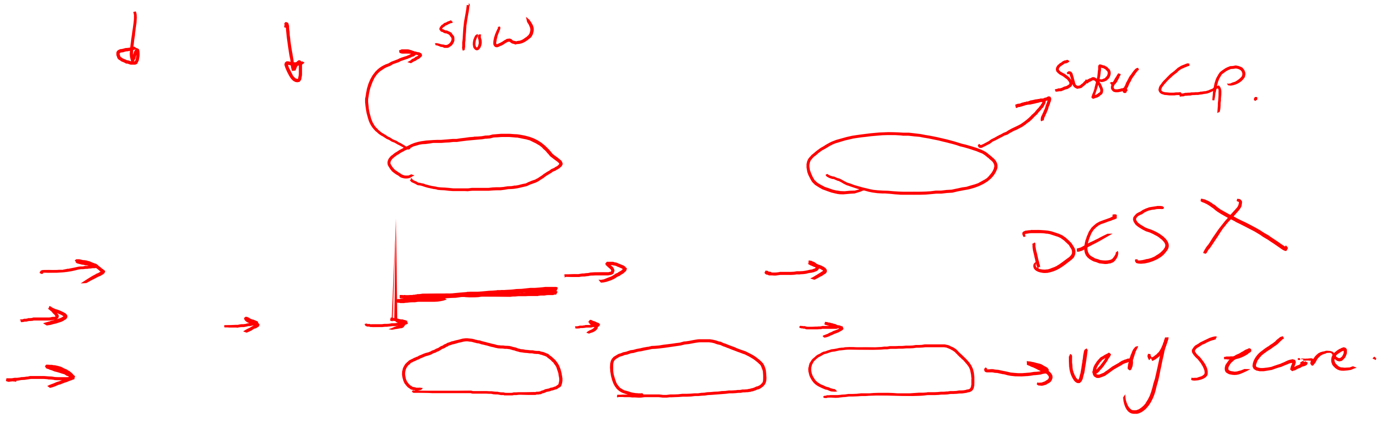
Brute Force Attack

- Approach: try all keys in key space
- Metric: number of operations (time)
- k bit key requires 2^k operations
- Depends on key length and computer speed

Cryptanalysis

- Approach: Find weaknesses in algorithms
- Methods: Linear cryptanalysis, differential cryptanalysis, meet-in-the-middle attack, side-channel attacks . . .
- Metrics:
  - Number of operations ✓
  - Amount of memory ✓
  - Number of known plaintexts/ciphertexts ✓

Brute Force Attacks on Symmetric Key Encryption



$2^{56} = 7.2 \times 10^{16}$

$10^9 = 72057594$ sec to conduct Brute force attack

Key length	Key space	Worst case time at speed:		
		10^9/sec	10^{12}/sec	10^{15}/sec
32	2^{32}	4 sec	4 ms	4 us
56	2^{56}	833 days	20 hrs	72 sec
64	2^{64}	584 yrs	213 days	5 sec
128	2^{128}	10^{22} yrs	10^{19} yrs	10^{16} yrs
192	2^{192}	10^{41} yrs	10^{38} yrs	10^{35} yrs
256	2^{256}	10^{60} yrs	10^{57} yrs	10^{54} yrs
26!	2^{88}	10^{10} yrs	10^{7} yrs	10^{4} yrs

$60 \times 60 \times 24$

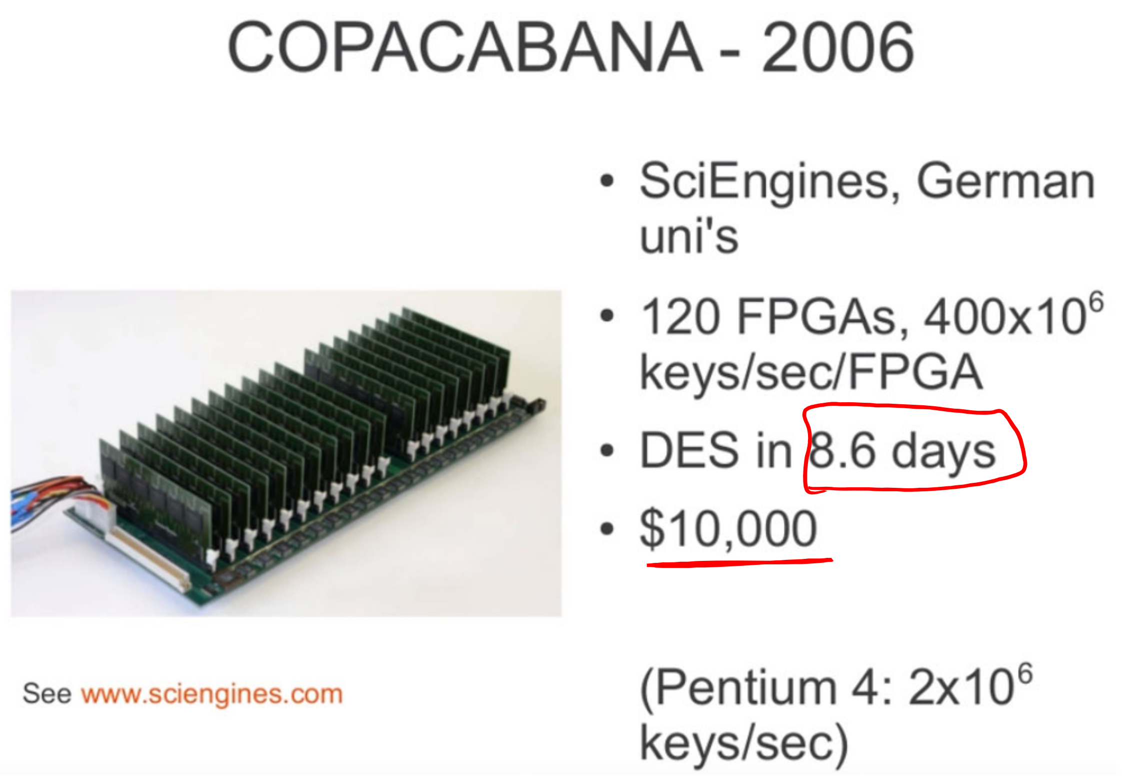
833.9 days

Brute Force Attacks on Symmetric Key Encryption

DeepCrack - 1998

- Developed by EFF
- < $250,000
- 80×10^9 keys/sec
- Solved DES challenge in 56 hours

Brute Force Attacks on Symmetric Key Encryption



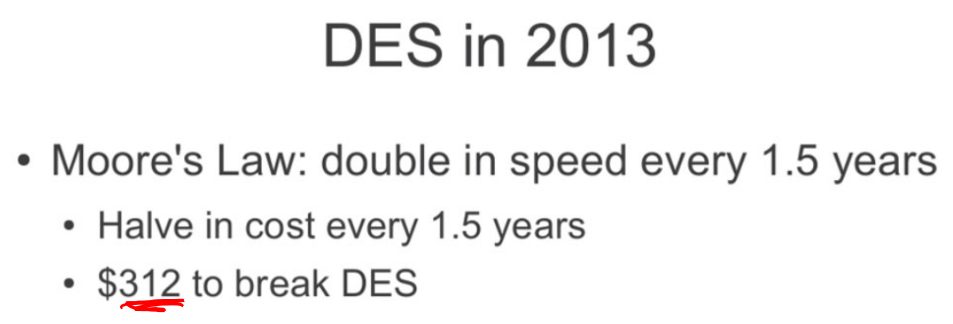
COPACABANA - 2006

- SciEngines, German uni's
- 120 FPGAs, 400x10^6 keys/sec/FPGA
- DES in 8.6 days
- $10,000

See www.sciengines.com

(Pentium 4: 2x10^6 keys/sec)

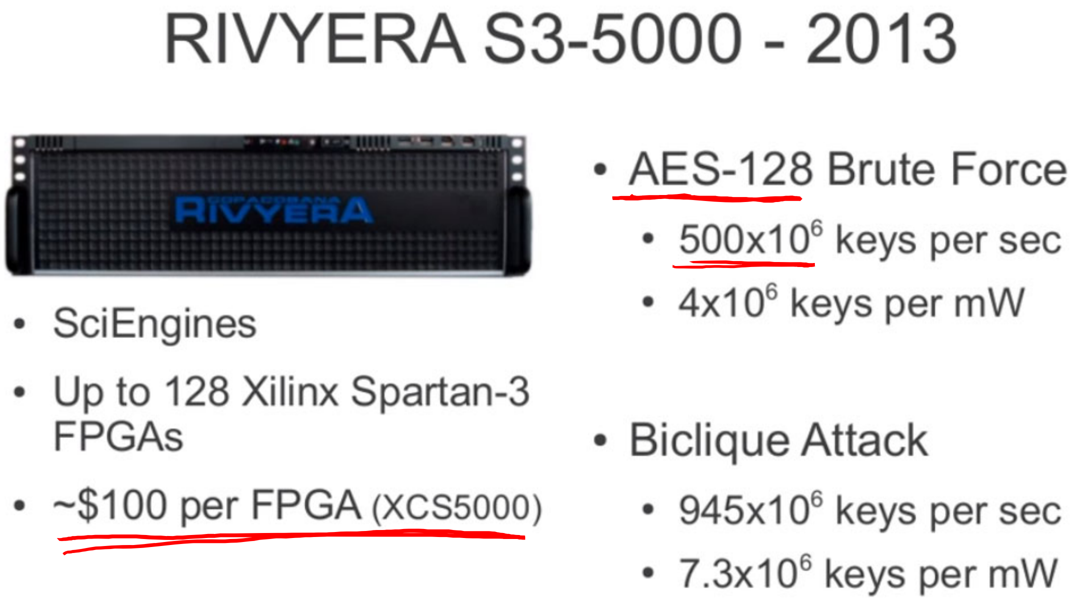
Brute Force Attacks on Symmetric Key Encryption



DES in 2013

- Moore's Law: double in speed every 1.5 years
  - Halve in cost every 1.5 years
  - $312 to break DES

Brute Force Attacks on Symmetric Key Encryption

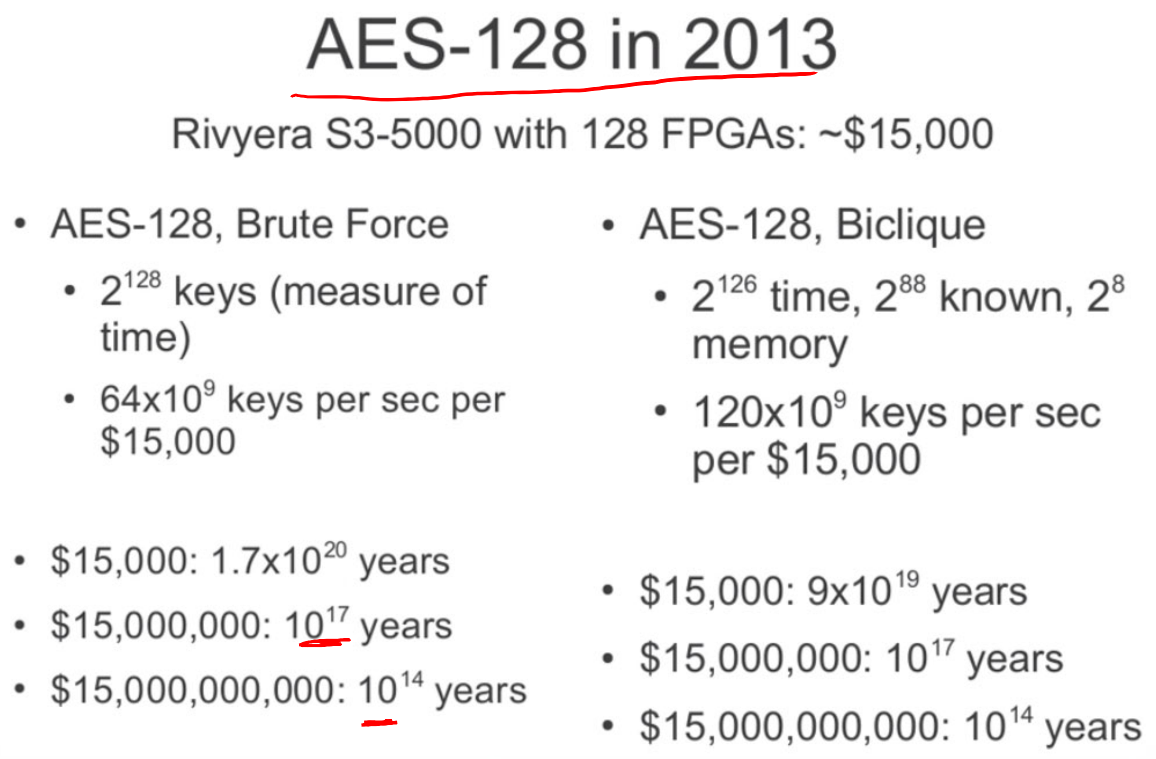


RIVYERA S3-5000 - 2013

- SciEngines
- Up to 128 Xilinx Spartan-3 FPGAs
- ~$100 per FPGA (XCS5000)

- AES-128 Brute Force
  - 500x10^{6} keys per sec
  - 4x10^{6} keys per mW
- Biclique Attack
  - 945x10^{6} keys per sec
  - 7.3x10^{6} keys per mW

Brute Force Attacks on Symmetric Key Encryption



AES-128 in 2013

Rivyera S3-5000 with 128 FPGAs: ~$15,000

- AES-128, Brute Force
  - 2^{128} keys (measure of time)
  - 64×10^{9} keys per sec per $15,000
- $15,000: 1.7×10^{20} years
- $15,000,000: 10^{17} years
- $15,000,000,000: 10^{14} years

- AES-128, Biclique
  - 2^{126} time, 2^{88} known, 2^{8} memory
  - 120×10^{9} keys per sec per $15,000
- $15,000: 9×10^{19} years
- $15,000,000: 10^{17} years
- $15,000,000,000: 10^{14} years

Video Summary

- What is symmetric key encryption
- Assumptions
- Symmetric key encryption algorithms (DES, 3DES, AES)
- Attacks on Encryption Algorithms