

# Cryptographic Algorithms and Key Size Issues

---

Çetin Kaya Koç  
Oregon State University, *Professor*  
<http://islab.oregonstate.edu/koc>  
[koc@ece.orst.edu](mailto:koc@ece.orst.edu)

# Overview

---

- Cryptanalysis Challenge
- Encryption:
  - DES → AES
- Message Digest Functions
  - MD5, SHA-1 → SHA-256, SHA-384, SHA-512
- Digital Signatures:
  - RSA, DSA → RSA, DSA, ECDSA
- Lenstra-Verheul Model for Key Sizes
- Mobile and Adhoc Network Challenge

# Cryptanalysis Challenge

---

- ❑ Advances in computer architecture for cryptanalysis
  - Special-purpose computers (DES breaking machine),
  - distributed computing
- ❑ Surprising algorithmic developments in cryptanalysis
  - Factoring, discrete log, elliptic curve discrete log, other methods for secret-key ciphers

# DES → AES

---

- ❑ DES is standardized (FIPS 46-3) in 1977
- ❑ Highly resistant to cryptanalytic attacks
- ❑ Became vulnerable to exhaustive key search attack in 1997
- ❑ Essentially broken in 1999
  - Using special hardware and software with an investment of \$250K, one can search 90B keys per second, breaking DES in 56 hours
- ❑ DES is still used in legacy systems

# DES → AES

---

- ❑ NIST started a process (competition) to replace DES with AES in Sep 1997
- ❑ Of 21 submissions, 15 were selected as AES candidates in Aug 1998
- ❑ 5 finalists were selected in Aug 1999
  - MARS, RC6, Rijndael, Serpent, Twofish
- ❑ Rijndael was selected as AES in Oct 2000
- ❑ AES became FIPS 197 in Nov 2001
- ❑ Triple DES (FIPS 46-3) is still a standard

# Advance Encryption Standard

---

- ❑ AES has three key sizes: 128, 192, 256
- ❑ Number of rounds: 10, 12, 14
- ❑ 128 bits is very strong
  - Assuming one can break DES in 1 second (trying  $2^{56}$  keys in one second), then, trying  $2^{128}$  keys requires 149 Trillion years
- ❑ AES Block size is 128 bits
- ❑ Large block size makes ECB a viable alternative
- ❑ AES is based on finite-field arithmetic  $GF(2^8)$ , but, table-lookup approaches are possible
- ❑ Security assurances for 20 years

# MD5, SHA-1 → new SHAs

---

- ❑ MD5 was proposed by Rivest, part of RSA Security PKCS
  - MD5: 128-bit message digest function
- ❑ SHA-1 was proposed by NIST, together with DSA
  - SHA-1: 160-bit message digest function
- ❑ MD5 and SHA are based on the same principles
- ❑ Hash functions attacks are different from the attacks on ciphers

# MD5, SHA-1 $\rightarrow$ new SHAs

---

- Collision (birthday) attacks on hash functions:

$$H(m_1) = H(m_2) \quad \text{but} \quad m_1 \neq m_2$$

- If  $r = \sqrt{2\lambda n}$  tries can be made on a hash function of  $n$  possible values, then a collision can be found with probability

$$1 - e^{-\lambda}$$

- Apply this rule to MD5:  $n=2^{128}$
- If we make

$$r = \sqrt{2 \cdot 32 \cdot 2^{128}} = 2^{67}$$

tries, then we will find a collision with probability

$$1 - e^{-32} \cong 1$$

- Hash functions of 128 bits or less are not secure

# MD5, SHA-1 → new SHAs

---

- SHA-1 is 160 bits .. still fine
- NIST introduced 3 new SHA functions
  - SHA-256, SHA-384, and SHA-512
- They are not direct generalizations of SHA
- Based on some new methods and constructs
- Standardized on Aug 2002 (FIPS 180-2)
  - SHA-1, SHA-256, SHA-384, SHA-512
- Some security issues
  - More security analyses are needed
  - Usage of truncated hashes needs clarification

# MD5, SHA-1 → new SHAs

---

## Properties of SHA functions

	Message	Block	Word	Digest	Security
SHA-1	$2^{64}$	512	32	160	80
SHA-256	$2^{64}$	512	32	256	128
SHA-384	$2^{128}$	1024	64	384	192
SHA-512	$2^{128}$	1024	64	512	256

# RSA, DSA → RSA, DSA, ECDSA

---

- ❑ RSA has been de facto digital signature method for enterprise networks
- ❑ DSA was first proposed in 1991
- ❑ DSA became a US standard in Dec 1998 (FIPS 186-1)
- ❑ In Feb 2000, FIPS 186-2 was published, making RSA, DSA, and ECDSA as US standards
- ❑ DSA prime is recommended to be 1024 bits
- ❑ Subgroup prime is 160 bits, same as SHA-1 size

# RSA, DSA $\rightarrow$ RSA, DSA, ECDSA

---

- ❑ ECDSA is based a set of fixed curves
- ❑ Curves over  $GF(p)$  have bit sizes
  - $|p| = 192, 224, 256, 384, 521$
- ❑ Curves over  $GF(p)$  are selected with special primes, allowing faster arithmetic
  - $p=2^{192}-2^{64}-1$
- ❑ Curves over  $GF(2^k)$  have bit sizes
  - $k = 163, 233, 283, 409, 571$
- ❑ Curves over  $GF(2^k)$  are both kind
  - random and Koblitz
- ❑ Normal basis and polynomial basis arithmetic are allowed for  $GF(2^k)$  fields

# Lenstra-Verheul Model

---

- Lenstra and Verheul built a model for estimating the key sizes for cryptographic functions
  - Ciphers, hash functions, and digital signatures
  - The model is supposed to be valid for many (25) years
- The model is based on *Gordon Moore Law*
  - Popular interpretation: Computing power per computer doubles every 18 months
  - Technology interpretation: Density of components per IC doubles every 18 months
  - Cost interpretation: Computing power and RAM which can be purchased per dollar doubles every 18 months

# DES, AES – Exhaustive Key Search

---

- ❑ Best method to break DES was exhaustive key search
- ❑ New cipher algorithms are not weaker, in fact, stronger due to advanced research
- ❑ Assumptions: New attacks will not be faster than exhaustive key search
- ❑ Similar arguments for Message Digest
- ❑ Warning: Avoid unknown, less-studied methods

# RSA - Factoring

---

- ❑ Public exponent should not be too small
- ❑ Breaking RSA is equivalent to factoring
- ❑ Many methods are developed, continuously improved
- ❑ There is a lot of room for progress
- ❑ More RAM is available for sieving
- ❑ New proposals for factoring hardware

# DH, DSA – Discrete Logarithms

---

- ❑ Large prime divisor of  $p-1$  is needed
- ❑ Not much algorithmic progress since Pollard rho algorithm
- ❑ Parallelization was proposed
- ❑ Slow progress is assumed

# ECC – Elliptic Curve Discrete Log

---

- ❑ Not much progress in elliptic curve discrete logarithm problem since 1985
- ❑ Bad curves need to be avoided
- ❑ Randomly picked curves over  $GF(p)$  with randomly picked prime  $p$  look good
- ❑ A large prime divides group order
- ❑ Substantial progress would be *catastrophic*

# Key-Size Estimates

---

Year	Enc	Hash	RSA	DSAsig	ECC
2002	72	144	1028	127	135
2005	74	148	1149	131	139
2010	78	156	1369	138	146
2015	82	164	1613	145	154
2020	86	172	1882	151	160

# Budget & Years

---

Year	Budget for attack in 1 day	Years on a low-budget Pentium
2002	\$160 M	48 M
2005	\$196 M	226 M
2010	\$277 M	3 B
2015	\$392 M	45 B
2020	\$555 M	654 B