RSA Key Sizes

Asia PKI Consortium GA/SC Meeting 2010
New Delhi

C.E.Veni Madhavan

Informatics Laboratory
Department of Computer Science and Automation
Indian Institute of Science, Bangalore
cevm@csa.iisc.ernet.in

29 October, 2010

Contents

- **1. Cryptography Primer**
- **2. Algorithms Engineering**
- **3. Cryptanalysis**
- **4. Cryptanalysis Techniques and Effort**
- **5. Typical work factors**
- **6. Attacks**

1. Cryptography Primer

- Combinatorial, Algebraic and Number Theoretic techniques
- Pseudo-random Bits
- Block and Stream Ciphers
- Public Key Encryption
- Digital signatures
- Hash functions and information integrity
- Challenge-Response, Zero Knowledge based identification
- Efficient implementation of protocols in software and hardware
- Technology of secure smart-card processors
- Key establishment, certification, escrow, TTP
- Cryptanalysis and Security of cryptographic protocols
- Patents, Export control laws, Standards and Cyber laws

Typical PIV 3 GHz, Linux, C Benchmarks :

- Stream Ciphers ($\simeq$1.5 Gbits/sec) :
  LFSR, non-linear FSR, FISH, PIKE, A5 ...
- Block Ciphers ($\simeq$300 Mbits/sec) :
  DES, IDEA, BLOWFISH, RC5 (64 bit); RC6, TWOFISH, MARS, RIJNDAEL, SERPENT (AES-128 bit)
- Public Key Ciphers ($\simeq$20 Kbits/sec) :
  RSA, ElGamal ($\mathbf{F}_p; \mathbf{F}_q, q = 2^n, p^n$), Elliptic Curve ($\mathbf{E}(\mathbf{F_q})$);
  Chor-Rivest, NTRU ...
- Digital Signatures
  (generation $\simeq$20 Kbits/sec, verification $\simeq$ 1.2 Mbits/sec) :
  RSA, ElGamal ($\mathbf{F}_p; \mathbf{F}_q, q = 2^n, p^n$), Elliptic Curve ($\mathbf{E}(\mathbf{F_q})$);

3. Cryptanalysis

1. **Integer Factoring Problems (IFP)** Let N be an integer with $N = p * q$ for prime integers, p, q. Given N find the factors.
2. **Discrete Logarithm Problems (DLP)** Let G be a group. The groups to be considered are (i) the multiplicative group of the finite field $\mathbf{F}_q$, for q an odd prime or $q = 2^m$, (ii)the additive group of points on an elliptic curve over a finite field $E(F_q)$. Let g be a fixed, distinguished element (e.g.,a generator of a cyclic group or an element of large order) of G and let $a = g^x$ for some x. Given g, a in G determine x.
3. **Statistical Analysis Problems (SAP) - cryptanalysis** Given the cipher-text $c =< c_0, \ldots, c_N >, c_j \in \{0, 1\}$ output of (i) a stream cipher or (ii) a block cipher, determine the corresponding (i) plain-text $p =< p_o, \ldots, p_N, p_j \in \{0, 1\} >$ or, (ii) symmetric key $k =< k_o, \ldots, k_n, k_j \in \{0, 1\} >$, under various cryptanalytic scenarios .

Cryptanalysis Techniques and Effort

- **Stream Ciphers :**
  linear complexity profile, correlations, mul. var. poly. eqns ...
- **Block Ciphers :**
  differential, linear, Mod n **attacks ...**
- **Public Key Ciphers integer factorization, discrete logarithms in groups, lattice short vectors, modular square roots ...**
- **side channel attacks - timing attacks, power analysis ...**
- **1 Day** $= 86400 >\sim 2^{16}$ **seconds; 1 Year** $= 2^{25}$ **seconds,**
- **(assuming 1 single precision int/float mul instruction = 1 cycle);**
  1 MIPS/ 1 Mflops Year $= 2^{45}$ **cycles ;**
  1 BIPS/ 1 Gflops Year $= 2^{55}$ **cycles ;**
  1 TIPS/ 1 Tflops Year $= 2^{65}$ **cycles ;**
  1 PIPS/ 1 Pflops Year $= 2^{75}$ **cycles ;**

Cryptanalysis Techniques and Effort

- **Our PC is 1GHz Pentium IV processor** $= 2^{30}$ **cycles/second ; 1 PC Year** $= 2^{55}$ **cycles;**
- **a desk-top super-computer delivers** $\simeq 2^{40}$ **cycles/second or** $\simeq 2^{65} cycles/year$ **- a PARAM-PADMA year (approximately the work-factor for factoring a 512 bit integer or breaking a RSA-512 key)**
- **DES (i) brute-force :** 2^{55} **trials X** 2^{9} **cycles per trial** $= 2^{64}$ **cycles** $= 512$ **BIPS Years or** $=$ **512 PC Years**
- **Assuming Differential Cryptanalysis implementation with all the required storage and communication, the effort is** 2^{45} **trials or** 2^{54} **cycles or 0.5 PC Year**

Cryptanalysis Techniques and Effort

- **Let** $L(n) = \exp\{(1.93 + o(1))(\log n)^{1/3}(\log\log n)^{2/3}\}$
- $L(n)$ **represents the cost of all computations for the currently, known, most efficient algorithms for Factoring, DL etc.**
- **The [1999] factoring record RSA155 (512 bit** $n = pq$ **), would thus be** $L(2^{2^9}) \sim 2^{64}$**. In actual practice it was** 2^{58}**, that is 64 times faster than straight DES attack. I call this equivalent to 1/64 DES cracks.**
- **I must note that certain arithmetic ops in factoring require more cycles than DES ops.**

5. Typical Work Factors

```
Integer factoring :
size (bits)                     512     1024     2048
work (cycles)                 2^{64}   2^{86}   2^{116}

Discrete logarithm in F_q
size (bits)                     512     1024     2048
work (cycles)                 2^{60}   2^{80}   2^{100}

Discrete logarithm in E(F_q), J(F_q)
size (bits)                     160     200      240
work (cycles)                 2^{70}   2^{90}   2^{120}

DES (16 rounds)  key size 56 bits
work (straight) : 2^{65} cycles
work (DC/LC   ) : 2^{55} cycles

AES (Rijndael - 10 rounds)  key size 128 bits
work :  > 2^{110} cycles
```

```
most stream ciphers key material (~128 bits)
work :  > 2^{110} cycles
```

Transposition cipher

size (chars)	400	900	1600
work (cycles)	2^{50}	2^{56}	2^{59}

```
[1995]
RSA-130 : 432 : exp( 1.93 * 6.69 * 3.19 )
        = exp(41.18) = 2^(59.41)

[1999]
RSA-512 : 512 : exp( 1.93 * 7.08 * 3.25 )
        = exp(44.10) = 2^(63.62)

[2003]
RSA-576 : 576 : exp( 1.93 * 7.36 * 3.30 )
        = exp(46.88) = 2^(67.6)

[2005]
RSA-640 : 640 : exp( 1.93 * 7.63 * 3.34 )
        = exp(49.18) = 2^(70.85)

[2010]
RSA-768 : 768 : exp( 1.93 * 8.10 * 3.40 )
        = exp(53.23) = 2^(76.80)
```

```
L(n,c,e)=exp{c*(ln n)^(1/3)*(ln(ln (n)))^(1/3),
c = 1.923, e=1/3
no. bits          u           practical bounds
                              T  = 2 ^ ( u ):

 463  61.11   54 (13000 hrs.@3GHz:~2^(57)>~2^(54))
 512  63.62   56.3 (?)
 576  67.67   58.9 (?)
 640  70.85   62 (40 Opteron,1yr:~40*3*2^(30)*2^(25))
 704  73.45   65.5 (?)(~11.3*40  = 452 Opteron yrs)
 768  76.80   69.3 (?)(~13.93*452=6296 Opteron yrs)
              ([7 Jan 2010] 2100 AMD64 years)
1024  86.76   (1 million AMD64 years)
2048 116.88   (billion-million AMD64 years)
```

6. Attacks

- **small exponents**
- **common modulus**
- **timing analysis**
- **simple power analysis**
- **diffeential power analysis**
- **fault injections**
- **branch predictions**
- **accelerators: cluster, FPGA, GPU**
- **quantum computers**