

# Computational Complexity of Cryptanalysis Problems

National seminar on e-security education  
through e-learning, e-learn '2007

14 December 2007

C-DAC, Noida C.E. Veni Madhavan

Dept. of Computer Science and Automation  
Indian Institute of Science, Bangalore  
Email : [cevm@csa.iisc.ernet.in](mailto:cevm@csa.iisc.ernet.in)

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

# 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

## 2. Algorithms Engineering

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 (  $F_p; F_q, q = 2^n, p^n$  ), Elliptic Curve (  $E(F_q)$  );  
Chor-Rivest, NTRU ...
- Digital Signatures  
( generation  $\simeq 20$  Kbits/sec, verification  $\simeq 1.2$  Mbits/sec ) :  
RSA, ElGamal (  $F_p; F_q, q = 2^n, p^n$  ), Elliptic Curve (  $E(F_q)$  );  
blind, undeniable, group ...
- Mitsubishi Smart card M16C - 16bit, 10MHz, 64KB ROM,  
4KB RAM 400 msec RSA Verification ( 1024 bit modulus,  
 $e = 65537$  )

- **Hyper-elliptic Curves, Jacobian and Abelian Varieties, Number Fields**
- **math. and algorithms**
- **integer primality proof**
- **integer factorization**
- **public key cryptosystems : NTRU, XTR, HFE, ...**
- **hard problems in arithmetic algebraic geometry**

## 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  $F_q$ , 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  $c = \langle c_0, \dots, c_N \rangle, c_j \in \{0, 1\}$  output of (i) a stream cipher or (ii) a block cipher, determine the corresponding (i) plain-text  $p = \langle p_0, \dots, p_N, p_j \in \{0, 1\} \rangle$  or, (ii) symmetric key  $k = \langle k_0, \dots, k_n, k_j \in \{0, 1\} \rangle$ , under various cryptanalytic scenarios .
4. *Statistical Analysis Problems (SAP) - steganalysis* Given a stego image  $S$ , determine with high levels of statistical significance, (1) the presence, (ii) the length of embedded content (iii) the location of embedding and (iv) the embedded content

## Quadratic Congruence Methods *Algorithm - Dixon*

1. **Build the prime base** ,  $P = \{p_1, \dots, p_{\pi(v)}\}$ , **where**  $\pi(v)$  **is the number of primes below**  $v$ .
2. **Pick a random**  $z, 1 \leq z \leq n - 1$  **and let**  $w = z^2 \pmod{N}$ .
3. **Factorize**  $w$  **over the prime base**  $P$ . **Let**  $w = W \times \prod p_i^{\alpha_i}$ .
4. **if**  $W \neq 1$ , **then goto Step2 else accumulate sufficient number** ( say,  $\pi(v) + 1$  ) **of factorizations and store the vectors**  $\gamma = (\gamma_1, \dots, \gamma_{\pi(v)+1})$  **where**  $\gamma$  **represents the parity vector of the exponents,**  $\gamma_i \equiv \alpha_i \pmod{2}$ . **Perform Gaussian elimination mod 2 on the parity vectors**  $\gamma$  **to get a zero vector.**
5. **if no nontrivial combination is generated in Step4 then goto Step2 else compute**  $y$  **as the product of prime powers obtained in Step4 and let**  $x$  **equal the product of the corresponding**  $z$ .
6. **if**  $x \not\equiv \pm y \pmod{N}$  **then compute**  $\gcd(x \pm y, N)$  **and HALT else delete the "first**  $w$  **and goto Step2**

- **Best known heuristics have either exponential or sub-exponential time complexity in size of input  $(\ln n)$  given by**

$$L[n, \gamma, c] = O\left(\exp((c + o(1))(\ln n)^\gamma (\ln \ln n)^{1-\gamma})\right),$$

**Here  $1 < c \leq 2$  and  $0 < \gamma \leq 1$ .**

- **Random Squares, Quadratic Sieve :  $\gamma = 1/2$ .  
Number Field Sieve :  $\gamma = 1/3$ .**

## 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  $\approx$   $2^{16}$  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;**
- **Our super computer PARAM-PADMA 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  $L(2^{29}) \sim 2^{64}$ . 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. So this scaling is actually not right.

Typical Work factors for known *best* heuristics

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]

$$\begin{aligned} \text{RSA-130} & : 432 : \exp( 1.93 * 6.69 * 3.19 ) \\ & = \exp(41.18) = 2^{(59.41)} \\ & : 2^{\{59\}} < L(n, 1/3, 1.93) < 2^{\{60\}} \end{aligned}$$

[1999]

$$\begin{aligned} \text{RSA-512} & : 512 : \exp( 1.93 * 7.08 * 3.25 ) \\ & = \exp(44.10) = 2^{(63.62)} \\ & : 2^{\{63\}} < L(n, 1/3, 1.93) < 2^{\{64\}} \end{aligned}$$

[2003]

$$\begin{aligned} \text{RSA-576} & : 576 : \exp( 1.93 * 7.36 * 3.30 ) \\ & = \exp(46.88) = 2^{(67.6)} \\ & : 2^{\{67\}} < L(n, 1/3, 1.93) < 2^{\{68\}} \end{aligned}$$

[2005]

$$\begin{aligned} \text{RSA-640} & : 640 : \exp( 1.93 * 7.63 * 3.34 ) \\ & = \exp(49.18) = 2^{(70.85)} \\ & : 2^{\{70\}} < L(n, 1/3, 1.93) < 2^{\{71\}} \end{aligned}$$

$$L(n,c,e)=\exp\{c*(\ln n)^{(1/3)}*(\ln(\ln (n)))^{(1/3)},$$

$$c = 1.923, e=1/3$$

no. bits		u	practical bounds T = 2 ^ ( u ):
463	61.113070	54	(13000 hrs.@3GHz:~2^(57)>~2^(54))
512	63.929363	56.3	(?)
576	67.375411	58.9	(?)
640	70.599666	62	(40 Opteron, 1yr:~40*3*2^(30)*2^(25) (Bonn, Nov'05)
704	73.636428	65.5	(?)(~11.3*40 = 452 Opteron yrs)
768	76.512120	69.3	(?)(~13.93*452=6296 Opteron yrs)
1024	86.766145		
2048	116.883848		

# Benchmarks

- Based on the  $L(n)$  estimate, with the constant **1.93**, the no. of cycles for 512, 576, 640 bits would be  $2^{64}, 2^{67}, 2^{70}$ , respectively.
- Based on certain other recent improvements, the constant is **1.65**. With this the no. of cycles for 512, 576, 640 bits would be  $2^{53}, 2^{56}, 2^{59}$ , respectively. *We hope to do slightly better than these, for multiple- moduli factoring.*
- On this basis and some initial experiments it is *expected that our heuristics may lead to much fewer cycles than that predicted by the analytic estimates.* That is our algebraic sieving *may* be completed in about 1/128 of the  $2^{64}$  or about  $2^{57}$  cycles, (or about ONE PIV 3GHZ YEAR  $\equiv$  2 PARAM-PADMA DAYS)
- Estimated Time for RSA-640 challenge : **32 PARAM PADMA YEARS !!!**
- Our Goal : **ONE PARAM PADMA YEAR !!!**
- The cost of the required  $2^{27}$  relations at @1 p/relation can be met out of the (assumed) prize money of US \$20,000 offered for the RSA-640 Challenge!
- Similar benchmarks on a range of processors being compiled. The processors include PIV, Opteron, Itanium, Xeon, IBM Power, SP2, PARAM, CRAY etc, in a variety of 32 / 64 bit and cluster configurations

## Combinatorial Problems

1. graph  $G$  on large primes in candidate relations
2. 2, 3, 4 cycles in  $G$
3. matchings in a bipartite version of  $G$
4. use of information derived from items above in matrix compaction
5. densities of roots of polynomial  $f$  modulo primes in Factor Base corresponding to the first degree prime ideals
6. characterizations of number of roots in terms of coefficients of the polynomial  $f$