













































 					0						_
	Squa	re an	d Mul	tiply A	Algori	thm A	Algorit	hm			
		c ← 0; for i ≺	; a ← 1 ← k dov	vnto 0							
		ć	lo c←	$2 \times c$							
			d ←	$(d \times d)$	mod n						
			if	bi = 1							
				then	c ← c d ← (d	+ 1 × a) mo	od n				
		returr	ı d		- (-						
i	9	8	7	6	5	4	3	2	1	0	
b_i	1	0	0	0	1	1	0	0	0	0	
С	1	2	4	8	17	35	70	140	280	560	
d	7	49	157	526	160	241	298	166	67	1	







■ P1	rogress in F	actorization	n [Table 9	.3]
	e		L	-
umber of Decimal	Approximate	Date Achieved	MIPS-years	Algorithm
Digits	Number of Bits	Aneil 1001	7	anadratic sieve
100	352	April 1991 April 1902	75	quadratic sieve
110	10.2	April 1992	15	quadratic sieve
110	308	June 1003	830	anadeatic sieve
110 120 129	398 428	June 1993 April 1994	830 5000	quadratic sieve
110 120 129 130	398 428 431	June 1993 April 1994 April 1996	830 5000 1000	quadratic sieve quadratic sieve seneralized number field sieve
110 120 129 130 140	398 428 431 465	June 1993 April 1994 April 1996 February 1999	830 5000 1000 2000	quadratic sieve quadratic sieve generalized number field sieve generalized number field sieve



