10. Kick-Off for Hash Functions

0 1 2 3 4 5 6

a b c d e f g h i j k l m n o p q r s t u

7 8

v w x y z.

255.

256

26通.

+0

250

0 1 2 3 4 5 6 7 8 9.

a: op

b: 10.

c: 20.

d:

z: 250.

a b c d e f g h i j k l m

n o p q r s t u v w x y z.

0 1 2 3 4

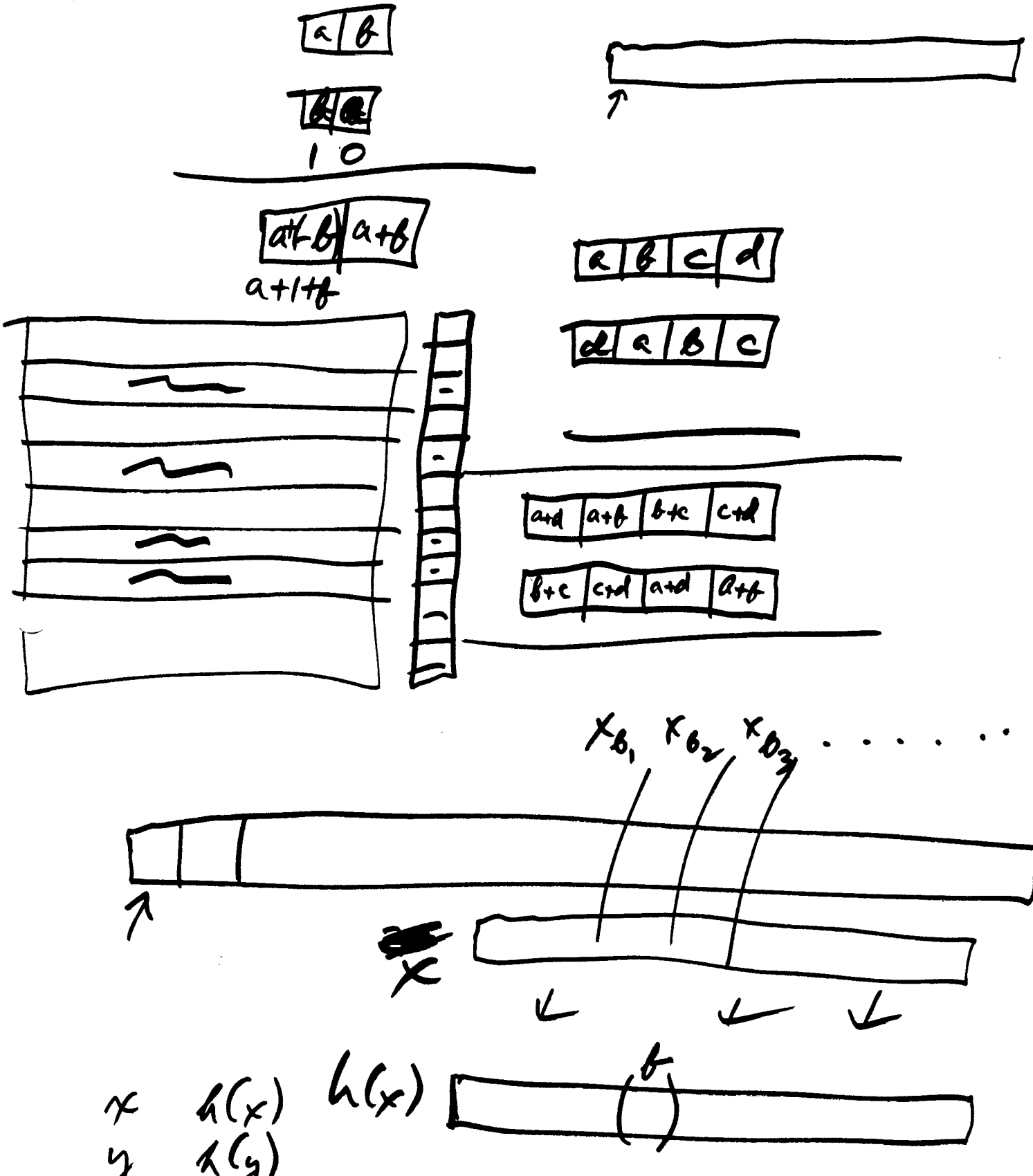
a b c d e f g h i j k l m

5 6 7 8 9

n o p q r s t u v w x y z

2nd chars

Good!

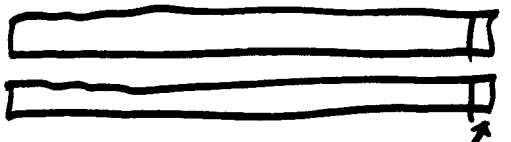

a b
1 0
a+b a+b
a+1+b
a b c d
d a b c
a+d a+b b+c c+d
b+c c+d a+d a+b
x_{b_1} x_{b_2} x_{b_3} . . . . . .
x
x h(x) h(x)
y r(y)

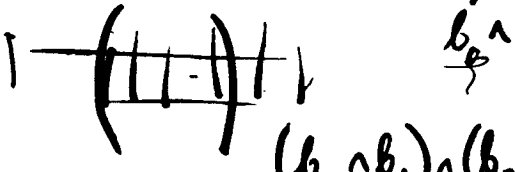
32 bit quantity N

1
3
7
15
31
63
127

N := N EOR (ROR(N,1))
N := N EOR (ROR(N,3))
N := N EOR (ROR(N,7))
N := N EOR (ROR(N,15))
N := N EOR (ROR(N,31))
N := N EOR (ROR(N,63))
N := N EOR (ROR(N,127))

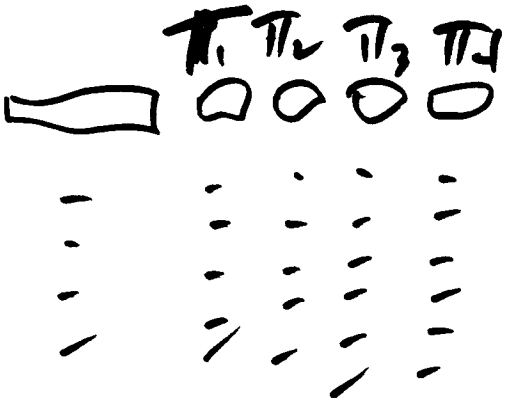
& | ^

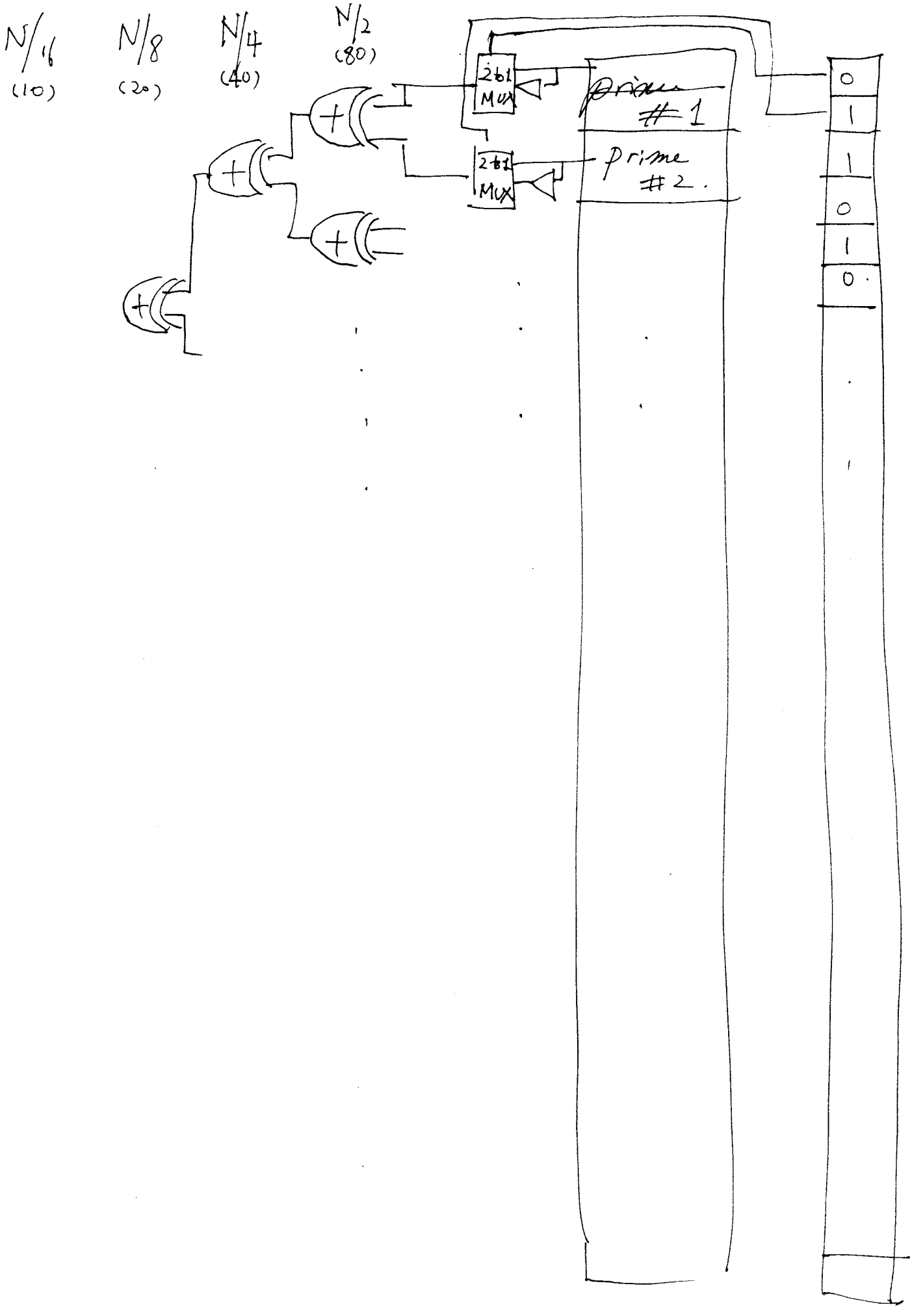




$(b_0 \wedge b_1) \wedge (b_3 \wedge$

$((b_0 \wedge b_1) \wedge (b_3 \wedge b_4)) \wedge ((b_7 \wedge b_8) \wedge (b_{10} \wedge$




N/16
(10)
N/8
(20)
N/4
(40)
N/2
(80)
2 bit MUX
2 bit MUX
prime #1
prime #2.
0
1
1
0
1
0

$2^9 \sim 2^8$

$2^6 = 64$

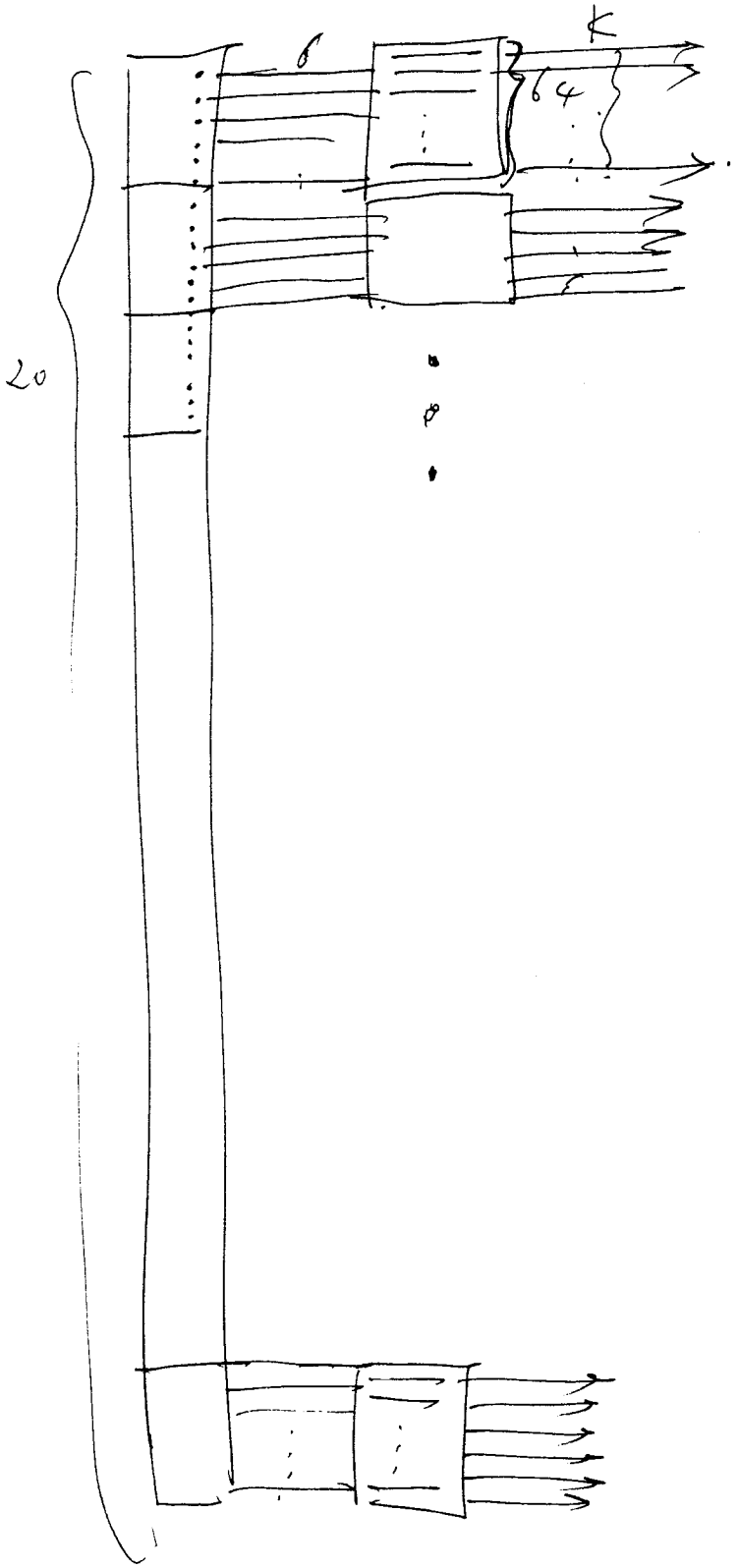
$2^7 \cdot 2^8$

2^k = table size.

256 → 8 bit

20 10 5 2 1

(5)

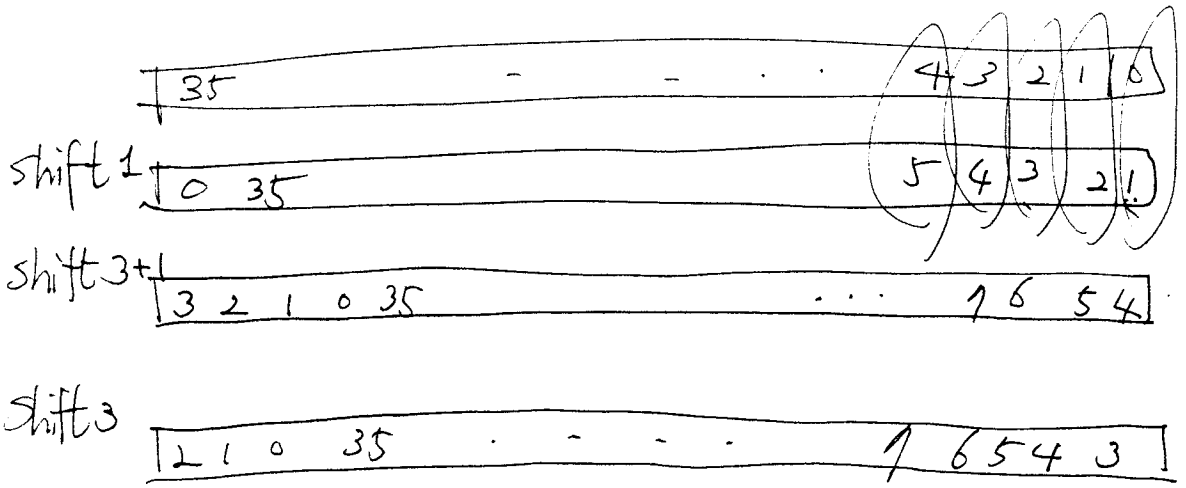


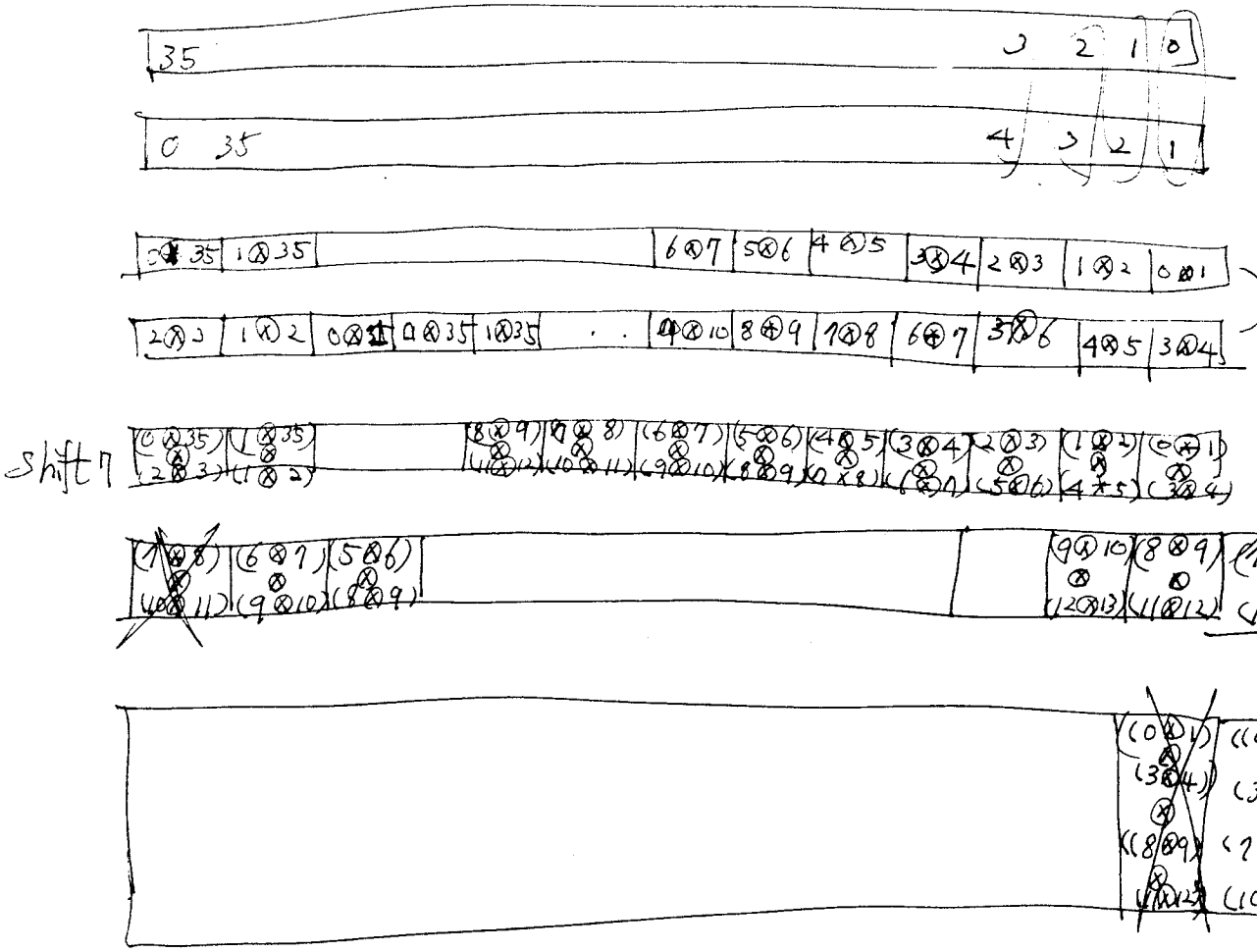
6k prime #

1024.

10000 0000 → 8 bit

1111 1111 → 256


35
4 3 2 1 0
shift 1
0 35
5 4 3 2 1
shift 3+
3 2 1 0 35
16 54
shift 3
2 1 0 35
1 6 5 4 3


35
3 2 1 0
0 35
4 3 2 1
shift 7

p	p	p	p	p	p	p	p	p	p	p	p
3	5	1187	1321	2687	3041	4463	4789	6043	6521	7867	8269
7	29	1223	1361	2707	3049	4483	4801	6047	6529	7883	8329
23	41	1283	1381	2767	3061	4507	4861	6067	6569	7907	8369
43	61	1303	1409	2803	3089	4523	4889	6143	6581	7927	8389
47	89	1307	1429	2843	3109	4547	4909	6163	6661	7963	8429
67	101	1327	1481	2887	3121	4567	4969	6203	6689	8087	8461
83	109	1367	1489	2903	3169	4583	5009	6247	6701	8123	8501
103	149	1423	1549	2927	3181	4603	5021	6263	6709	8147	8521
107	181	1427	1601	2963	3209	4643	5081	6287	6761	8167	8581
127	229	1447	1609	3023	3221	4663	5101	6323	6781	8243	8609
163	241	1483	1621	3067	3229	4703	5189	6343	6829	8263	8629
167	269	1487	1669	3083	3301	4723	5209	6367	6841	8287	8641
223	281	1523	1709	3163	3329	4783	5261	6427	6869	8363	8669
227	349	1543	1721	3167	3361	4787	5281	6547	6949	8387	8681
263	389	1567	1741	3187	3389	4903	5309	6563	6961	8423	8689
283	401	1583	1789	3203	3449	4943	5381	6607	7001	8443	8741
307	409	1607	1801	3307	3461	4967	5441	6703	7069	8447	8761
347	421	1627	1861	3323	3469	4987	5449	6763	7109	8467	8821
367	449	1663	1889	3343	3529	5003	5501	6803	7121	8527	8849
383	461	1667	1901	3347	3541	5023	5521	6823	7129	8543	8861
443	509	1723	1949	3407	3581	5087	5569	6827	7229	8563	8929
463	521	1747	2029	3463	3701	5107	5581	6863	7309	8623	8941
467	541	1783	2069	3467	3709	5147	5641	6883	7321	8627	8969
487	569	1787	2081	3527	3761	5167	5669	6907	7349	8647	9001
503	601	1823	2089	3547	3769	5227	5689	6947	7369	8663	9029
523	641	1847	2129	3583	3821	5303	5701	6967	7481	8707	9041
547	661	1867	2141	3607	3881	5323	5741	6983	7489	8747	9049
563	701	1907	2161	3623	3889	5347	5749	7027	7529	8783	9109
587	709	1987	2221	3643	3929	5387	5801	7043	7541	8803	9161
607	761	2003	2269	3727	3989	5407	5821	7103	7549	8807	9181
643	769	2027	2281	3767	4001	5443	5849	7127	7561	8863	9209
647	809	2063	2309	3803	4021	5483	5861	7187	7589	8867	9221
683	821	2083	2341	3823	4049	5503	5869	7207	7621	8887	9241
727	829	2087	2381	3847	4129	5507	5881	7243	7649	8923	9281
743	881	2143	2389	3863	4201	5527	5981	7247	7669	8963	9341
787	929	2203	2441	3907	4229	5563	6029	7283	7681	9007	9349
823	941	2207	2521	3923	4241	5623	6089	7307	7741	9043	9421
827	1009	2243	2549	3943	4261	5647	6101	7487	7789	9067	9461
863	1021	2267	2609	3947	4289	5683	6121	7507	7829	9103	9521
883	1049	2287	2621	3967	4349	5743	6221	7523	7841	9127	9601
887	1061	2347	2689	4003	4409	5783	6229	7547	7901	9187	9629
907	1069	2383	2729	4007	4421	5807	6269	7583	7949	9203	9649
947	1109	2423	2741	4027	4441	5827	6301	7603	8009	9227	9661
967	1129	2447	2749	4127	4481	5843	6329	7607	8069	9283	9689
983	1181	2467	2789	4243	4549	5867	6361	7643	8081	9323	9721
1063	1201	2503	2801	4283	4561	5903	6389	7687	8089	9343	9749
1087	1229	2543	2861	4327	4621	5923	6421	7703	8101	9403	9769
1103	1249	2647	2909	4363	4649	5927	6449	7723	8161	9463	9781
1123	1289	2663	2969	4423	4721	5987	6469	7727	8209	9467	9829
1153	1301	2683	3001	4447	4729	6007	6481	7823	8221	9547	9901