

Lecture 8 March 29, 2023

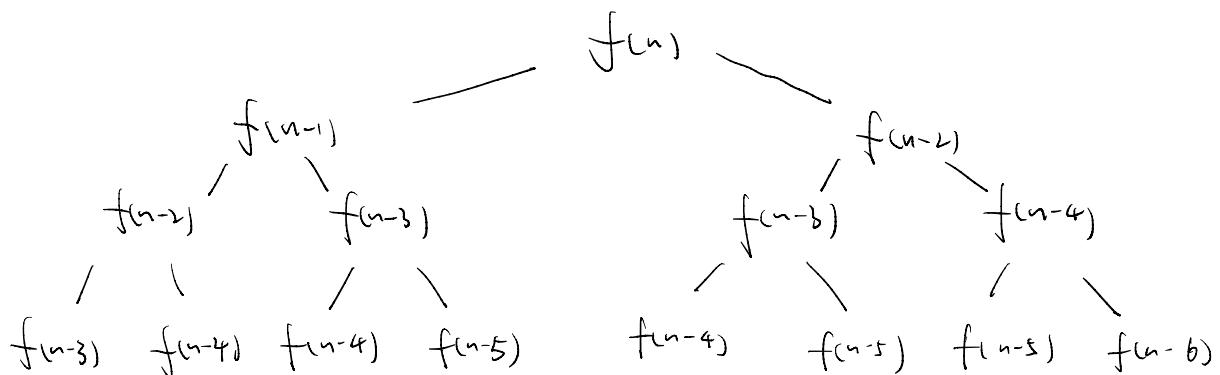
$$1 \ 1 \ 2 \ 3 \ 5 \ 8 \ 13$$

$$f(n) = f(n-1) + f(n-2)$$

$f_5(n)$ ↗

```
if ((n==0) || (n==1))
    return 1
return (f(n-1) + f(n-2));
```

↓



$$T[0] = 1 \quad T[2-n] = -1$$

$$T[1] = 1$$

\downarrow
 $f_5(n)$ ↗

```
if T[n] != -1
    return T[n]
return fib(n-1) + fib(n-2)
```

$$T[n] = fib(n-1) + fib(n-2)$$

return $T[n]$

Longest Common Subsequence Leetcode 11 43.

	- A	C	G	G	C	S	T
-	0 0	0 0	0 0	0 0	0 0	0 0	0 0
A	0 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1
T	0 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1	1 1 → 1
Y	0 1	2 2 → 2	2 2 → 2	2 2 → 2	2 2 → 2	2 2 → 2	2 2 → 2
C	0 1	2 2 → 3	3 3 → 3	3 3 → 3	3 3 → 3	3 3 → 3	3 3 → 3
G	0 1	2 3 → 3	3 4 → 4	4 4 → 4	4 4 → 4	4 4 → 4	4 4 → 4
S	0 1	2 3 → 3	3 4 → 4	4 5 → 5	5 5 → 5	5 5 → 5	5 5 → 5
T	0 1	2 3 → 3	3 4 → 4	4 5 → 5	5 6 → 6	6 6 → 6	6 6 → 6

if ($y_i == x_j$) $T[i-1, j-1] + 1$

else $\max[T[i-1, j], T[i, j-1]]$

ADD + DELETE

Edit Distance: Levenshtein Edit Distance

*	- A	C	G	G	C	S	T
*	0 1 2 3 4 5 6 7						
A	1 0 → 1 → 2 → 3 → 4 → 5 → 6						
T	2 1 1 2 3 4 5 5						
C	3 2 1 2 3 3 4 5						
G	4 3 2 1 → 2 3 4 5						
S	5 4 3 2 1 2 3 4						
T	6 5 4 3 2 2 2 3						
T	7 6 5 4 3 3 3 2						

Add

Delete

Substitute.

if ($y_i == x_j$) $\min(T[i-1, j] + 1, T[i, j-1] + 1, T[i-1, j-1])$

else $\min(T[i-1, j] + 1, T[i, j-1] + 1, T[i-1, j-1] + 1)$

Knapsack

Value	10	40	30	50
weight	5	4	3	3
	I ₁	I ₂	I ₃	I ₄

weight I can take

	I ₁	I ₁ +I ₂	I ₁ +I ₂ +I ₃
0	0	0	0
1	0	0	0
2	0	0	0
3	0	0	30
4	0	40	40
5	10	40	40
6	10	40	40
7	10	40	70
8	10	40	70
9	10	50	70
10	10	50	70

value

weight 3

Carry weight

	Value for items 1 to 3	Value for items 1 to 4
0	\$0	
1	\$1	
2	\$8	
3	\$10	
4	\$11	
5	\$18	\$18
6	\$19	
7	\$19	
8	\$19	

Item #4
Weight I₄.W = 4 lbs
and has value I₄.V = \$12

If I can carry W=5 lbs, should I take item #4?
If I don't take it, I can keep the \$18 from items 1-3.
If I do take it, I have 1 lb left over from which I can get \$1 Value from 1-3

Formula: Max (T[Prev, W], T[PrevCol, W-I₄.W] + I₄.V)

For w=6: Max (18 or 12+1) - Don't Take I₄ for 5 lbs.

If w=6 lbs Max (19, 12+8) \Rightarrow Take I₄

item #1 item #2 item #3 item #4

weight(lb)	2	3	1	4
value(\$)	8	10	1	12

item #1, #2, #3, #4 only have one

carry weight	Value for item 1	Value for items 1 and 2	Value for items 1 to 3	Value for items 1 to 4
0	0	0	0	0
1	0	0	1	1
2	8	8	8	8
3	8	10	10	10
4	8	10	11	12
5	8	18	18	18
6	8	18	19	20
7	8	18	19	22
8	8	18	19	23

Formula: Max (T[Prev, w], T[Prev Col, W - I4.w] + I4.w])

3 six-sided die {1, 2, 3, 4, 5, 6}

六面骰子

$$6^3 = \geq 16 \text{ rolls possible.}$$

sum die:	1	2
0	0	0
1	1	0
2	1	1
3	1	2
4	1	3
5	1	4
6	1	5
7	0	6
8	0	5
9	0	4
10	0	3
11	0	2
12	0	1
13	0	0
14	0	0
15	0	0

prev Dice	Current Die
2	1
3	2 ways \times 1 way 1 1 way \times 1 way 2 } = 2 ways
4	3 ways \times 1 way 1 2 ways \times 1 way 2 } = 3 ways 1 way \times 1 way 3 }
5	4
6	3
7	2
8	1
9	4
10	3
11	2
12	1
13	5
14	4
15	3
16	2
17	1
18	5
19	4
20	3
21	2
22	1
23	6
24	5
25	4
26	3
27	2
28	1
29	7
30	6
31	5
32	4
33	3
34	2
35	1
36	8
37	7
38	6
39	5
40	4
41	3
42	2
43	1
44	9
45	8
46	7
47	6
48	5
49	4
50	3
51	2
52	1
53	10
54	9
55	8
56	7
57	6
58	5
59	4
60	3
61	2
62	1
63	11
64	10
65	9
66	8
67	7
68	6
69	5
70	4
71	3
72	2
73	1
74	12
75	11
76	10
77	9
78	8
79	7
80	6
81	5
82	4
83	3
84	2
85	1
86	13
87	12
88	11
89	10
90	9
91	8
92	7
93	6
94	5
95	4
96	3
97	2
98	1
99	14
100	13
101	12
102	11
103	10
104	9
105	8
106	7
107	6
108	5
109	4
110	3
111	2
112	1
113	15
114	14
115	13
116	12
117	11
118	10
119	9
120	8
121	7
122	6
123	5
124	4
125	3
126	2
127	1
128	16
129	15
130	14
131	13
132	12
133	11
134	10
135	9
136	8
137	7
138	6
139	5
140	4
141	3
142	2
143	1
144	17
145	16
146	15
147	14
148	13
149	12
150	11
151	10
152	9
153	8
154	7
155	6
156	5
157	4
158	3
159	2
160	1
161	18
162	17
163	16
164	15
165	14
166	13
167	12
168	11
169	10
170	9
171	8
172	7
173	6
174	5
175	4
176	3
177	2
178	1
179	19
180	18
181	17
182	16
183	15
184	14
185	13
186	12
187	11
188	10
189	9
190	8
191	7
192	6
193	5
194	4
195	3
196	2
197	1
198	20
199	19
200	18
201	17
202	16
203	15
204	14
205	13
206	12
207	11
208	10
209	9
210	8
211	7
212	6
213	5
214	4
215	3
216	2
217	1
218	21
219	20
220	19
221	18
222	17
223	16
224	15
225	14
226	13
227	12
228	11
229	10
230	9
231	8
232	7
233	6
234	5
235	4
236	3
237	2
238	1
239	22
240	21
241	20
242	19
243	18
244	17
245	16
246	15
247	14
248	13
249	12
250	11
251	10
252	9
253	8
254	7
255	6
256	5
257	4
258	3
259	2
260	1
261	23
262	22
263	21
264	20
265	19
266	18
267	17
268	16
269	15
270	14
271	13
272	12
273	11
274	10
275	9
276	8
277	7
278	6
279	5
280	4
281	3
282	2
283	1
284	24
285	23
286	22
287	21
288	20
289	19
290	18
291	17
292	16
293	15
294	14
295	13
296	12
297	11
298	10
299	9
300	8
301	7
302	6
303	5
304	4
305	3
306	2
307	1
308	25
309	24
310	23
311	22
312	21
313	20
314	19
315	18
316	17
317	16
318	15
319	14
320	13
321	12
322	11
323	10
324	9
325	8
326	7
327	6
328	5
329	4
330	3
331	2
332	1
333	26
334	25
335	24
336	23
337	22
338	21
339	20
340	19
341	18
342	17
343	16
344	15
345	14
346	13
347	12
348	11
349	10
350	9
351	8
352	7
353	6
354	5
355	4
356	3
357	2
358	1
359	27
360	26
361	25
362	24
363	23
364	22
365	21
366	20
367	19
368	18
369	17
370	16
371	15
372	14
373	13
374	12
375	11
376	10
377	9
378	8
379	7
380	6
381	5
382	4
383	3
384	2
385	1
386	28
387	27
388	26
389	25
390	24
391	23
392	22
393	21
394	20
395	19
396	18
397	17
398	16
399	15
400	14
401	13
402	12
403	11
404	10
405	9
406	8
407	7
408	6
409	5
410	4
411	3
412	2
413	1
414	29
415	28
416	27
417	26
418	25
419	24
420	23
421	22
422	21
423	20
424	19
425	18
426	17
427	16
428	15
429	14
430	13
431	12
432	11
433	10
434	9
435	8
436	7
437	6
438	5
439	4
440	3
441	2
442	1
443	30
444	29
445	28
446	27
447	26
448	25
449	24
450	23
451	22
452	21
453	20
454	19
455	18
456	17
457	16
458	15
459	14
460	13
461	12
462	11
463	10
464	9
465	8
466	7
467	6
468	5
469	4
470	3
471	2
472	1
473	31
474	30
475	29
476	28
477	27
478	26
479	25
480	24
481	23
482	22
483	21
484	20
485	19
486	18
487	17
488	16
489	15
490	14
491	13
492	12
493	11
494	10
495	9
496	8
497	7
498	6
499	5
500	4
501	3
502	2
503	1
504	32
505	31
506	30
507	29
508	28
509	27
510	26
511	25
512	24
513	23
514	22
515	21
516	20
517	19
518	18
519	17
520	16
521	15
522	14
523	13
524	12
525	11
526	10
527	9
528	8
529	7
530	6
531	5
532	4
533	3
534	2
535	1
536	33
537	32
538	31
539	30
540	29
541	28
542	27
543	26
544	25
545	24
546	23
547	22
548	21
549	

sum die:	1	2	3		15	prev Dice	Current Die
0	0	0					
1	1	0				14 0	1 ↗ 1
2	1	1				13 0	1 ↗ 2
3	1	2				12 1 x 1 ↗ 3	= 1
4	1	3				11 2 x 1 ↗ 4	= 2
5	1	4				10 3 x 1 ↗ 5	= 3
6	1	5				9 4 x 1 ↗ 6	= 4
7	0	6					
8	0	5					
9	0	4					
10	0	3					
11	0	2					
12	0	1					
13	0	0					
14	0	0					
15	0	0			10		

Greatest common divisor (GCD)

$$\text{GCD}(18, 12) = 6$$

$$\text{GCD}(641, 23) = \left\lfloor \frac{641}{23} \right\rfloor = 27 \quad 641 \% 23 = 20$$

$\text{GCD}(23, 20)$

$$\text{GCD}(20, 3)$$

$$\text{GCD}(3, 1)$$

$$\text{GCD}(1, 0)$$

$$\alpha \quad \beta \quad \alpha \quad \beta \quad \alpha \quad \beta$$

$$-1 \quad \quad \quad \quad \quad 1 \quad 0$$

$$0 \quad 641 \quad 23 \quad 27 \quad 20 \quad 0 \quad 1$$

$$1 \quad 23 \quad 20 \quad 1 \quad 3 \quad 1 \quad -27$$

$$2 \quad 20 \quad 3 \quad 6 \quad 2 \quad -1 \quad 28$$

$$3 \quad 3 \quad 2 \quad 1 \quad 1 \quad 7 \quad -195$$

$$4 \quad 2 \quad \boxed{1} \quad 2 \quad 0 \quad -8 \quad 223$$

$$5 \quad \boxed{1} \quad 0 \quad - \quad - \quad 23 \quad -641$$

$$\beta_1 = \beta_{-1} - \beta_0 \alpha_0 \\ = 0 - 1 \times 27 \\ = -27$$

$$\alpha_1 = \alpha_{-1} - \alpha_0 \beta_0 \\ = 1 - 0 \cdot 27 \\ = 1$$

$$\alpha_k = \left\lfloor \frac{\alpha_{k-1}}{\beta_{k-1}} \right\rfloor$$

$$\beta_k = \beta_{k-1} - \beta_{k-1} \alpha_{k-1}$$

$$\boxed{\alpha_0 \cdot \alpha_k + \beta_0 \cdot \beta_k = \beta_k}$$

$$\alpha_k = \beta_{k-1}$$

$$\beta_k = \beta_{k-1}$$

$$-8 \times 641 + 23 \times 223 = 1$$

$$\boxed{\frac{1}{23} \% 641 = 223}$$

$$(23 \cdot 223) \% 641 = 1$$

$$\frac{1}{23} = 223$$

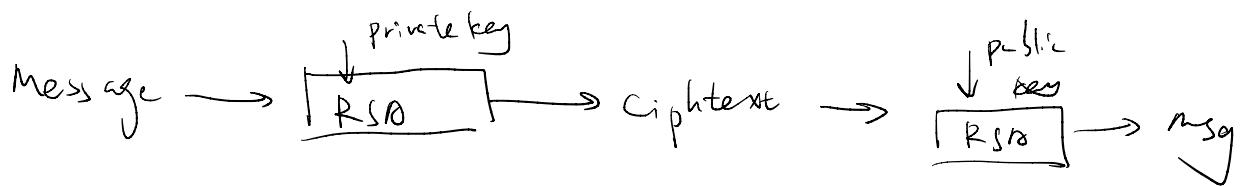
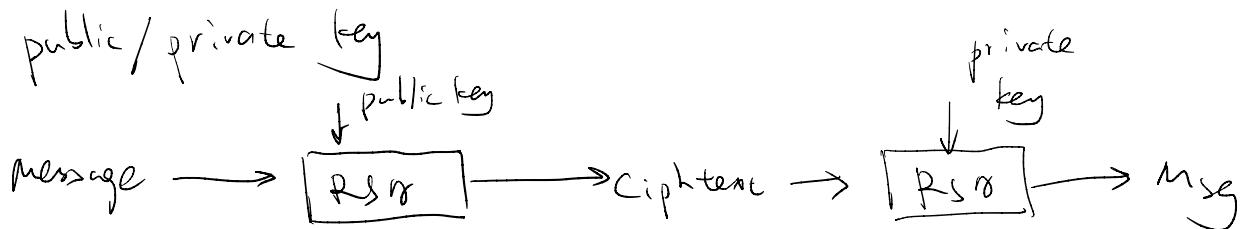
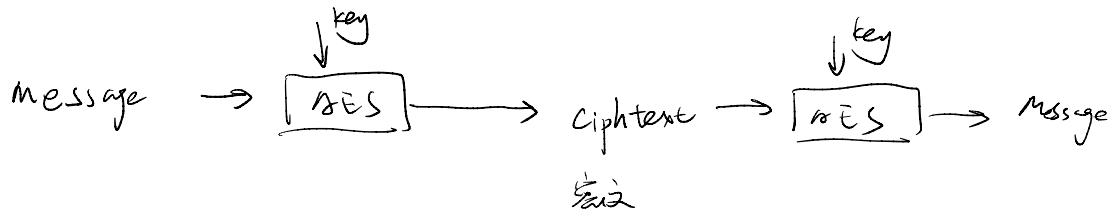
$$(-8 \cdot 641) \% 641 + (23 \cdot 223) \% 641 = 1 \% 641$$

$$0 + (23 \cdot 223) \% 641 = 1$$

A B Q R

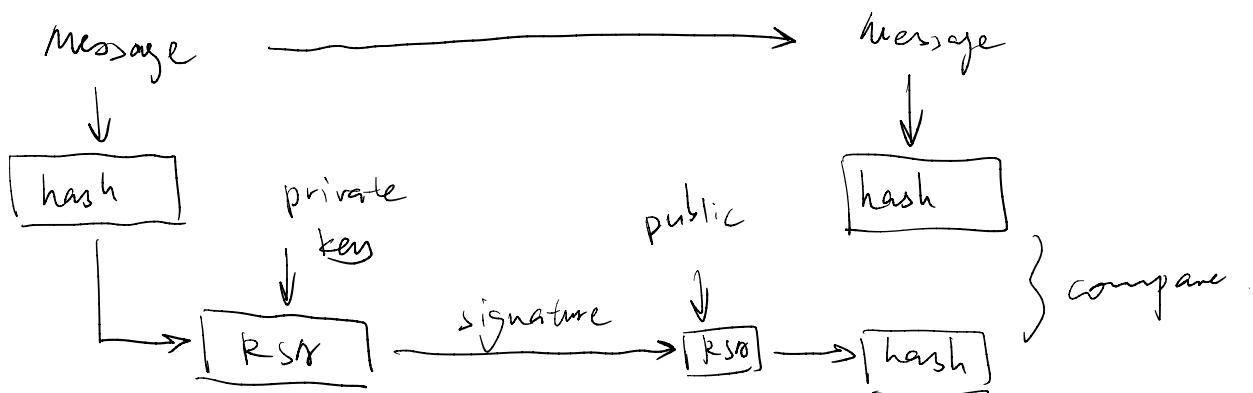
1				
2	18	12	1	b
1	12	\boxed{b}	2	0
2	\boxed{b}	0	—	—

Symmetric key cryptography



public / private key is expensive. Usually is not happen.

Normally what happen is this :



Message is a number

8 MB Message is a number with 64 million bits.

You would break it into "chunks")

32000 - 2k bit chunks.

public key (e, n) private key (d, n)

encrypt $\text{message}^e \% n = \text{ciphertext}$

Ciphertext $\% n =$ message

sign $\left(\begin{array}{c} \text{message} \\ \text{or} \\ \text{hash} \end{array} \right)^d \% n =$ ciphertext
signature

$$\begin{pmatrix} \text{ciphertext} \\ \text{signature} \end{pmatrix}^e \% n = \begin{pmatrix} \text{message} \\ \text{hash} \end{pmatrix}$$

$$M^{ed} \% n = M$$

$$M^{\phi(n)} \% n = 1$$

$$m^{\phi(n)+1} \% n = m \quad \text{and} \quad \phi(n) + 1$$

$$\text{ed \% } \phi(n) = 1$$

$$\sum \% \text{ of } 11 = 2$$

$$2\% \times 11 = 2$$

$$2^2 \cdot \% \cdot 11 = 2$$

$$2^{31} \% \approx 2$$

1. pick 2 prime numbers p, q
 2. calculate $\boxed{n} = p \cdot q$
 3. calculate $\phi(n) = (p-1)(q-1)$
 4. pick \boxed{e} such that $\text{gcd}(\phi(n), e) = 1$ and $1 < e < \phi(n)$
 5. calculate $\boxed{d} = \frac{1}{e} \% \phi(n)$
- public key = $\{e, n\}$
private key = $\{d, n\}$
- Forget p and q . If anybody figure out what p, q are, they can figure out what d is. So you got to lose p and q to protect d .

$$(m^e)^d = m \quad (m^d)^e \% n = m$$

$$c^{\boxed{d}} \% n = m$$

1. $p = 11$ $q = 17$
2. $n = 187$ $(11 \cdot 17)$
3. $\phi(n) = (p-1)(q-1) = 10 \cdot 16 = 160$
4. pick $e = 7$ public key $(7, 187)$
5. computed $d = \frac{1}{7} \% 160 = 23$ private key $(23, 187)$

α	β	γ	δ	ϵ	β
160	7	22	6	2	1
7	6	1	1	1	-12
6	1	6	0	-1	$\boxed{23}$

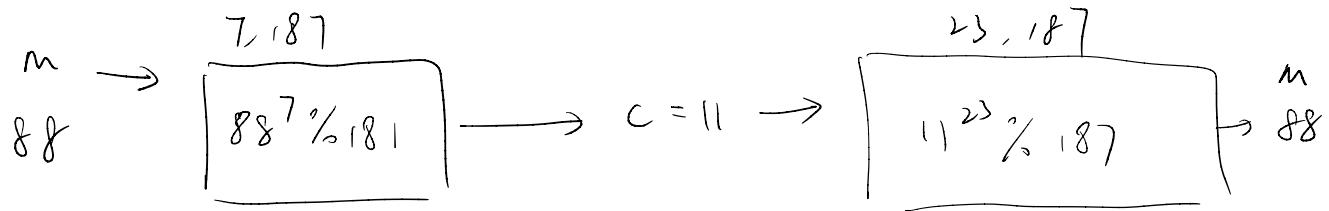
$$\frac{1}{7} \% 160 = 23$$

message = 88

$$88^7 \% 187 = 11$$

cipher + ext = 11

$$11^{23} \% 187 = 88$$

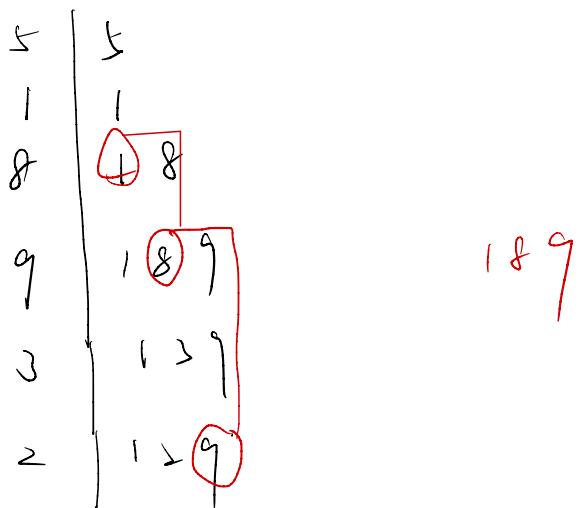


Test hit.

table row may be just few steps, not too complex.

Longest Increasing Subsequence

5 1 8 9 3 2



5 2 8 1 9 3

