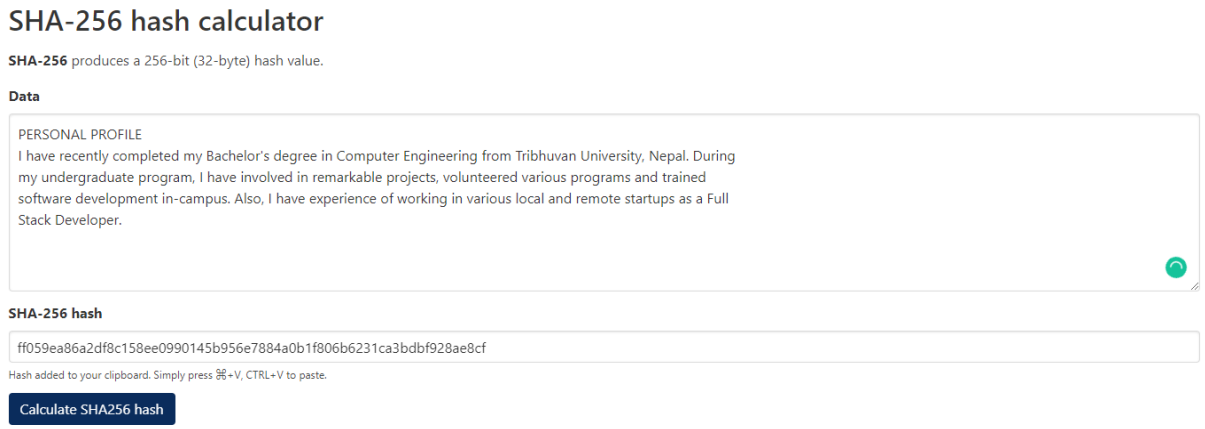
Homework for section 7 (due date tbd)

Question 1: Use on-line SHA-2 calculator:

a) Pick a portion of your resume

b) Hash it with SHA-2

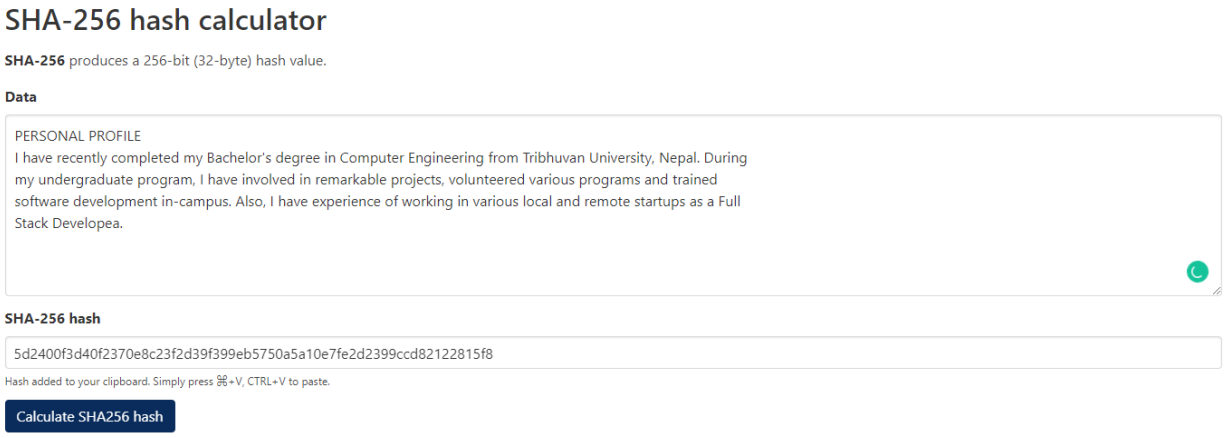


c) Modify one character

Modified last word with one character:

Developer to **Developea**

d) Hash it with SHA-2



f) Verify the differences in the resulting message digests

Two message digests are completely different with change in one character.

1st case: ff059ea86a2df8c158ee0990145b956e7884a0b1f806b6231ca3bdbf928ae8cf

2nd case: 5d2400f3d40f2370e8c23f2d39f399eb5750a5a10e7fe2d2399ccd82122815f8

Question 2: Create a blockchain

a) Segment parts of your resume in 3 blocks

Block 1:

PERSONAL PROFILE

I have recently completed my Bachelor's degree in Computer Engineering from Tribhuvan University, Nepal.

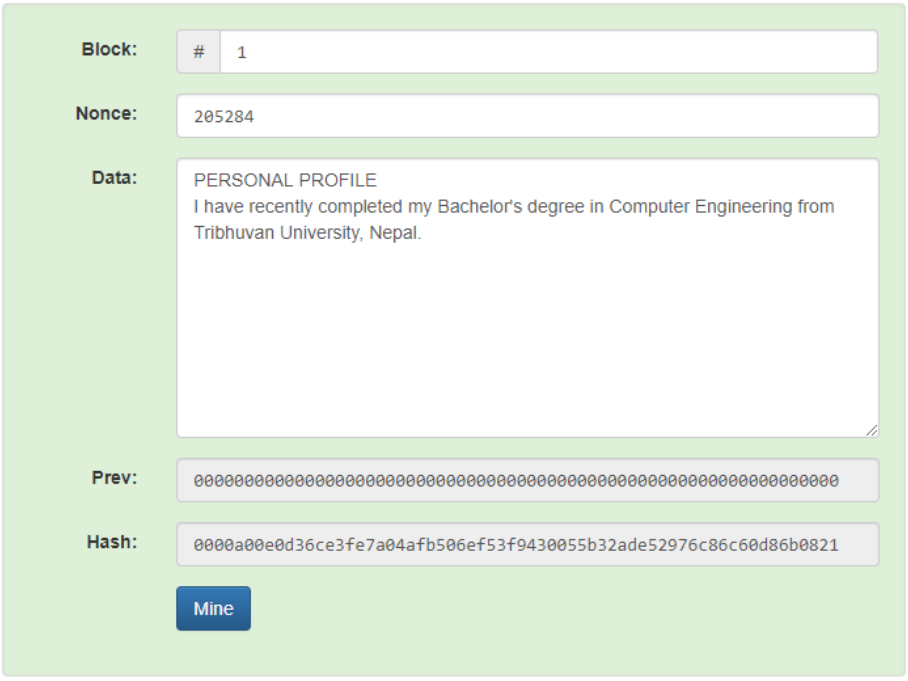
Block2:

During my undergraduate program, I have involved in remarkable projects, volunteered various programs and trained software development in-campus.

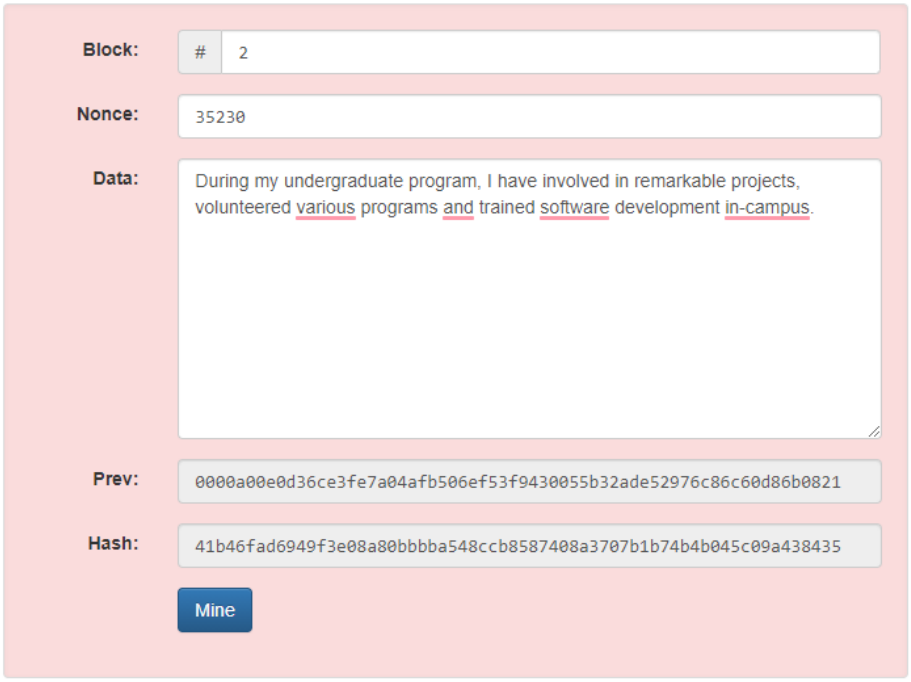
Block3:

Also, I have experience of working in various local and remote startups as a Full Stack Developer.

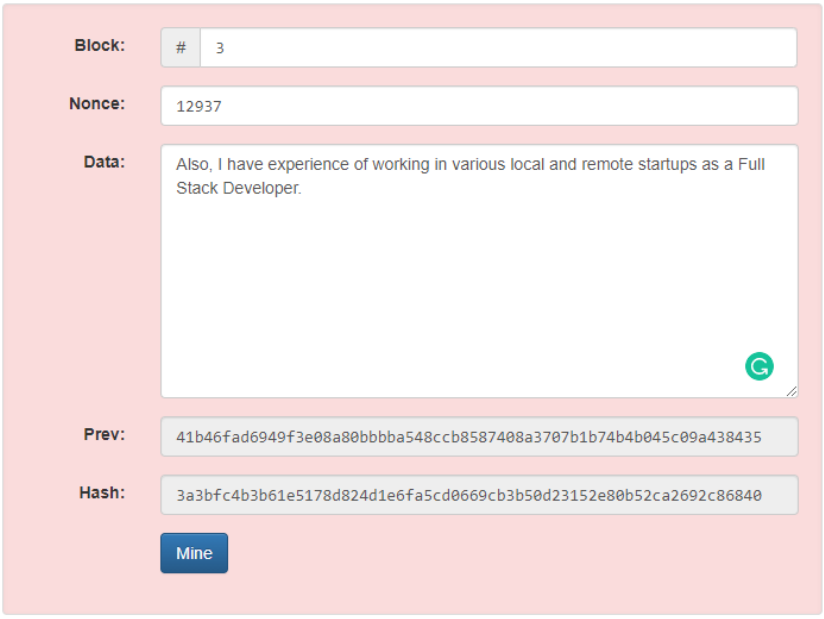
b) Hash the first part: H1



c) Hash (H1 + Part2): H2



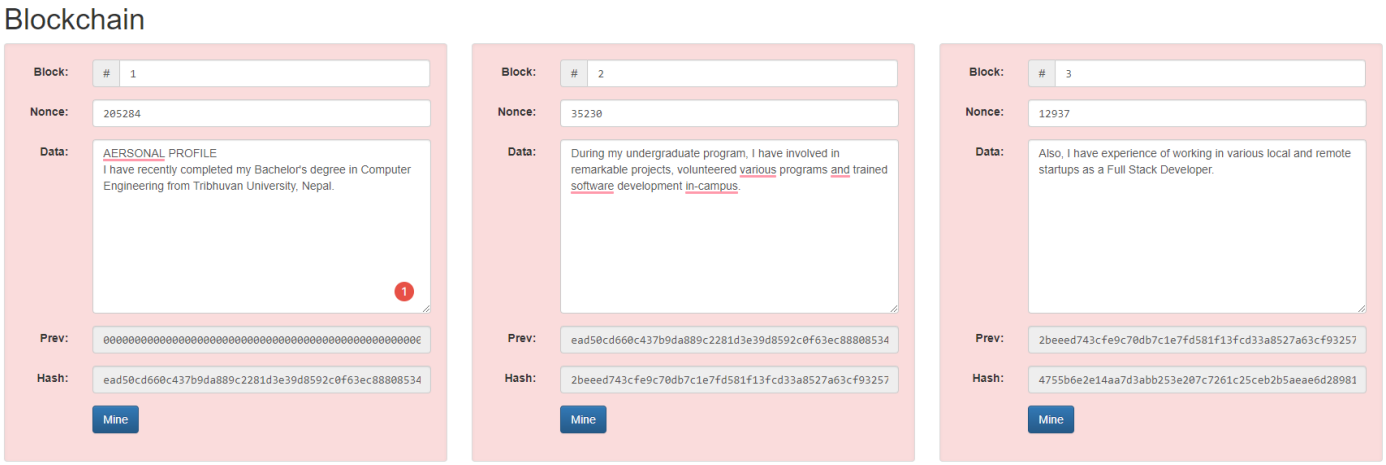
d) Hash (H2 + Part 3): H3



e) Modify one character to verify the resulting message digests

Changed one character of first word in block 1:

PERSONAL to **AERSONAL**



Message Digest has been completely changed.

Homework for section 8A - part 1 (due date tbd)

Use EA to find: gcd(9135,8070) and gcd(11296,8976)

gcd(9135,8070)

i	**ri-1**	**ri**	**qi**	**ri+1**
1	r0 = 9135	r1 = 8070	q1 = 1	r2 = 1065
2	r1 = 8070	r2 = 1065	q2 = 7	r3 = 615
3	r2 = 1065	r3 = 615	q3 = 1	r4 = 450
4	r3 = 615	r4 = 450	q4 = 1	r5 = 165
5	r4 = 450	r5 = 165	q5 = 2	r6 = 120
6	r5 = 165	r6 = 120	q6 = 1	r7 = 45
7	r6 = 120	r7 = 45	q7 = 2	r8 = 30
8	r7 = 45	r8 = 30	q8 = 1	r9 = 15
9	r8 = 30	**r9 = 15 = g**	q9 = 2	r10 = 0

gcd(11296,8976)

i	**ri-1**	**ri**	**qi**	**ri+1**
1	r0 = 11296	r1 = 8976	q1 = 1	r2 = 2320
2	r1 = 8976	r2 = 2320	q2 = 3	r3 = 2016
3	r2 = 2320	r3 = 2016	q3 = 1	r4 = 304
4	r3 = 2016	r4 = 304	q4 = 6	r5 = 192
5	r4 = 304	r5 = 192	q5 = 1	r6 = 112
6	r5 = 192	r6 = 112	q6 = 1	r7 = 80
7	r6 = 112	r7 = 80	q7 = 1	r8 = 32
8	r7 = 80	r8 = 32	q8 = 2	r9 = 16
9	r8 = 32	**r9 = 16 = g**	q9 = 2	r10 = 0

Homework for section 8A - part 2: **(Due date tbd)**

Find **S** and **T** for 11296 and 8976

i	R R_i	Q Q_i	S S_i	T T_i	EA $R_i = Q_{i+1}R_{i+1} + R_{i+2}$	EEA: S $S_i = S_{i-2} - Q_{i-1}\,S_{i-1}$	EEA: T $T_i = T_{i-2} - Q_{i-1}\,T_{i-1}$
0	R_0 = 11296	-	S_0 = **1**	T_0 = **0**	R0 = Q_1 R1 + R2 = (8976 * 1) + 2320		
1	R_1 = 8976	Q_1 =1	S_1 = **0**	T_1 = **1**	R1 = Q_2 R2 + R3 = (2320 * 3) + 2016		
2	R_2 = 2320	Q_2 =3	S_2 = 1	T_2 = -1	R2 = Q_3 R3 + R4 = (2016 * 1) + 304	S2 = S0 – Q_1 S1 = 1 – 1 * 0 = 1	T2 = T0 – Q_1 T1 = 0 – 1 * 1 = -1
3	R_3 = 2016	Q_3 = 1	S_3 = -3	T_3 = 4	R3 = Q_4 R4 + R5 = (304 * 6) + 192	S3 = S1 – Q_2 S2 = 0 – 3 * 1 = -3	T3 = T1 – Q_2 T2 = 1 – 3 * -1 = 4
4	R_4 = 304	Q_4 = 6	S_4 = 4	T_4 = -5	R4 = Q_5 R5 + R6 = (192 * 1) + 112	S4 = S2 – Q_3 S3 = 1 – 1 * -3 = 4	T4 = T2 – Q_3 T3 = -1 – 1 * 4 = -5
5	R_5 = 192	Q_5 = 1	S_5 = -27	T_5 = 34	R5 = Q_6 R6 + R7 = (112 * 1) + 80	S5 = S3 – Q_4 S4 = -3 – 6 * 4 = -27	T5 = T3 – Q_4 T4 = 4 – 6 * -5 = 34
6	R_6 = 112	Q_6 = 1	S_6 = 31	T_6 = -39	R6 = Q_7 R7 + R8 = (80 * 1) + 32	S6 = S4 – Q_5 S5 = 4 – 1 * -27 = 31	T6 = T4 – Q_5 T5 = -5 – 1 * 34 = -39
7	R_7 = 80	Q_7 = 1	S_7 = -58	T_7 = 73	R7 = Q_8 R8 + R9 = (32 * 2) + 16	S7 = S5 – Q_6 S6 = -27 – 1 * 31 = -58	T7 = T5 – Q_6 T6 = 34 – 1 * -39 = 73
8	R_8 = 32	Q_8 = 2	S_8 = 89	T_8 = -112	R8 = Q_9 R9 + R10 = (16 * 2) + 0	S8 = S6 – Q_7 S7 = 31 – 1 * -58 = 89	T8 = T6 – Q_7 T7 = -39 – 1 * 73 = -112
	g = 16		**S = -236**	**T = 297**		S9 = S7 – Q_8 S8 = -58 – 2 * 89 = -236	T9 = T7 – Q_8 T8 = 73 – 2 * -112 = 297

Homework for section 8B (due date tbd)

Fast Exponentiation 2273

2273	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	
squ		0											X x X
squ			0										X^2 x X^2
squ				0									X^4 x X^4
squ					0								X^8 x X^8
mul					1								X^{16} x X
squ						0							X^{17} x X^{17}
mul						1							X^{34} x X
squ							0						X^{35} x X^{35}
mul							1						X^{70} x X
squ								0					X^{71} x X^{71}
squ									0				X^{142} x X^{142}
squ										0			X^{284} x X^{284}
squ											0		X^{568} x X^{568}
squ												0	X^{1136} x X^{1136}
mul												1	**X^{2272} x X= X^{2273}**