Muhammad Izham Bin Norhamadi
B032020039 S2G1

Tutorial 9: Newton Polynomial Threshold Scheme

a) Master key K=139
b) Threshold Scheme using Newton Polynomial mod a prime P = 257. The policy is m = 5 of n = 8 shadow keys. Given the master key K as a_0. Set a polynomial of degree $m-1$ from coefficients $[a_0, a_1, a_2, \ldots, a_{m-1}]$ in Table 1 below.

i	0	1	2	3	4
a_i	K	19	23	29	43

Table 1: Secret coefficients of a master polynomial.

Generate n=8 shadow keys (x_i, y_i) for i= 0, 1, ..., $n-1$ from polynomial

$$A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{m-1} \cdot x^{m-1}$$

From $x_0, x_1, x_2, \ldots, x_{n-1}$, compute $y_0, y_1, y_2, \ldots, y_{n-1}$ by $y_i = A(x_i) \bmod P$.

i	0	1	2	3	4	5	6	7
x_i	3	5	7	9	11	13	15	17
y_i	43	212	224	121	9	58	245	97

Table 2: 8 Shadow keys are spread out.

c) Take the first 5 points of shadow key and build to a divided difference table.

i	x_i	y_i	y_i'	y_i''	y_i'''	$y_i^{(4)}$
0	3	y_0				
			y_{01}			
1	5	y_1		y_{02}		
			y_{12}		y_{03}	
2	7	y_2		y_{13}		y_{04}
			y_{23}		y_{14}	
3	9	y_3		y_{24}		
			y_{34}			
4	11	y_4				

Table 3: Generate a friendly divided difference table.

Muhammad Izham Bin Norhamadi
B032020039 S2G1

x_i	y_i	nume	deno		nume	deno		nume	deno		nume	deno	
3	43												
		-169	129	44									
5	212				-207	193	141						
		-12	129	251				59	43	224			
7	224				71	193	82				87	225	43
		103	129	180				51	43	137			
9	121				124	193	31						
		112	129	56									
11	9												

d) Generate a polynomial $P_{m-1}(x)$ via Newton interpolation.

$P_{m-1}(x) = y_0$
$+ y_{01}(x - x_0)$
$+ y_{02}(x - x_0)(x - x_1)$
$+ y_{03}(x - x_0)(x - x_1)(x - x_2)$
$+ y_{04}(x - x_0)(x - x_1)(x - x_2)(x - x_3)$

$P_4(x) = 43$
$+ 44 (x - 3)$
$+ 141 (x - 3)(x - 5)$
$+ 224 (x - 3)(x - 5)(x - 7)$
$+ 43 (x - 3)(x - 5)(x - 7)(x - 9)$

e) Evaluate the polynomial $P_{m-1}(x)$ at $x = 0$ to regenerate the master key K.

$P_4(x) = 43$
$+ 44 (0 - 3)$
$+ 141 (0 - 3)(0 - 5)$
$+ 224 (0 - 3)(0 - 5)(0 - 7)$
$+ 43 (0 - 3)(0 - 5)(0 - 7)(0 - 9) = 123 \pmod{257}$

Muhammad Izham Bin Norhamadi
B032020039 S2G1

Sample Solutions:

$A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_4 \cdot x^4$

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
4	173	185	82	227	19	206	58

Divided Difference Table

a_0	a_1	a_2	a_3	a_4	y_0	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_0	y_{01}	y_{02}	y_{03}	y_{04}
100	19	23	29	43	4	173	185	82	227	19	206	58	4	213	141	33	43
101	19	23	29	43	5	174	186	83	228	20	207	59	5	213	141	33	43
102	19	23	29	43	6	175	187	84	229	21	208	60	6	213	141	33	43
103	19	23	29	43	7	176	188	85	230	22	209	61	7	213	141	33	43
104	19	23	29	43	8	177	189	86	231	23	210	62	8	213	141	33	43
105	19	23	29	43	9	178	190	87	232	24	211	63	9	213	141	33	43
106	19	23	29	43	10	179	191	88	233	25	212	64	10	213	141	33	43
107	19	23	29	43	11	180	192	89	234	26	213	65	11	213	141	33	43
108	19	23	29	43	12	181	193	90	235	27	214	66	12	213	141	33	43
109	19	23	29	43	13	182	194	91	236	28	215	67	13	213	141	33	43
110	19	23	29	43	14	183	195	92	237	29	216	68	14	213	141	33	43
111	19	23	29	43	15	184	196	93	238	30	217	69	15	213	141	33	43
112	19	23	29	43	16	185	197	94	239	31	218	70	16	213	141	33	43
113	19	23	29	43	17	186	198	95	240	32	219	71	17	213	141	33	43
114	19	23	29	43	18	187	199	96	241	33	220	72	18	213	141	33	43
115	19	23	29	43	19	188	200	97	242	34	221	73	19	213	141	33	43
116	19	23	29	43	20	189	201	98	243	35	222	74	20	213	141	33	43
117	19	23	29	43	21	190	202	99	244	36	223	75	21	213	141	33	43
118	19	23	29	43	22	191	203	100	245	37	224	76	22	213	141	33	43
119	19	23	29	43	23	192	204	101	246	38	225	77	23	213	141	33	43
120	19	23	29	43	24	193	205	102	247	39	226	78	24	213	141	33	43
121	19	23	29	43	25	194	206	103	248	40	227	79	25	213	141	33	43
122	19	23	29	43	26	195	207	104	249	41	228	80	26	213	141	33	43
123	19	23	29	43	27	196	208	105	250	42	229	81	27	213	141	33	43
124	19	23	29	43	28	197	209	106	251	43	230	82	28	213	141	33	43
125	19	23	29	43	29	198	210	107	252	44	231	83	29	213	141	33	43
126	19	23	29	43	30	199	211	108	253	45	232	84	30	213	141	33	43
127	19	23	29	43	31	200	212	109	254	46	233	85	31	213	141	33	43
128	19	23	29	43	32	201	213	110	255	47	234	86	32	213	141	33	43
129	19	23	29	43	33	202	214	111	256	48	235	87	33	213	141	33	43
130	19	23	29	43	34	203	215	112	0	49	236	88	34	213	141	33	43
131	19	23	29	43	35	204	216	113	1	50	237	89	35	213	141	33	43

Muhammad Izham Bin Norhamadi
B032020039 S2G1

132	19	23	29	43	36	205	217	114	2	51	238	90	36	213	141	33	43
133	19	23	29	43	37	206	218	115	3	52	239	91	37	213	141	33	43
134	19	23	29	43	38	207	219	116	4	53	240	92	38	213	141	33	43
135	19	23	29	43	39	208	220	117	5	54	241	93	39	213	141	33	43
136	19	23	29	43	40	209	221	118	6	55	242	94	40	213	141	33	43
137	19	23	29	43	41	210	222	119	7	56	243	95	41	213	141	33	43
138	19	23	29	43	42	211	223	120	8	57	244	96	42	213	141	33	43
139	19	23	29	43	43	212	224	121	9	58	245	97	43	213	141	33	43
140	19	23	29	43	44	213	225	122	10	59	246	98	44	213	141	33	43
141	19	23	29	43	45	214	226	123	11	60	247	99	45	213	141	33	43
142	19	23	29	43	46	215	227	124	12	61	248	100	46	213	141	33	43
143	19	23	29	43	47	216	228	125	13	62	249	101	47	213	141	33	43
144	19	23	29	43	48	217	229	126	14	63	250	102	48	213	141	33	43
145	19	23	29	43	49	218	230	127	15	64	251	103	49	213	141	33	43
146	19	23	29	43	50	219	231	128	16	65	252	104	50	213	141	33	43
147	19	23	29	43	51	220	232	129	17	66	253	105	51	213	141	33	43
148	19	23	29	43	52	221	233	130	18	67	254	106	52	213	141	33	43
149	19	23	29	43	53	222	234	131	19	68	255	107	53	213	141	33	43
150	19	23	29	43	54	223	235	132	20	69	256	108	54	213	141	33	43
151	19	23	29	43	55	224	236	133	21	70	0	109	55	213	141	33	43
152	19	23	29	43	56	225	237	134	22	71	1	110	56	213	141	33	43
153	19	23	29	43	57	226	238	135	23	72	2	111	57	213	141	33	43
154	19	23	29	43	58	227	239	136	24	73	3	112	58	213	141	33	43
155	19	23	29	43	59	228	240	137	25	74	4	113	59	213	141	33	43
156	19	23	29	43	60	229	241	138	26	75	5	114	60	213	141	33	43
157	19	23	29	43	61	230	242	139	27	76	6	115	61	213	141	33	43
158	19	23	29	43	62	231	243	140	28	77	7	116	62	213	141	33	43
159	19	23	29	43	63	232	244	141	29	78	8	117	63	213	141	33	43
160	19	23	29	43	64	233	245	142	30	79	9	118	64	213	141	33	43
161	19	23	29	43	65	234	246	143	31	80	10	119	65	213	141	33	43
162	19	23	29	43	66	235	247	144	32	81	11	120	66	213	141	33	43
163	19	23	29	43	67	236	248	145	33	82	12	121	67	213	141	33	43
164	19	23	29	43	68	237	249	146	34	83	13	122	68	213	141	33	43
165	19	23	29	43	69	238	250	147	35	84	14	123	69	213	141	33	43
166	19	23	29	43	70	239	251	148	36	85	15	124	70	213	141	33	43
167	19	23	29	43	71	240	252	149	37	86	16	125	71	213	141	33	43
168	19	23	29	43	72	241	253	150	38	87	17	126	72	213	141	33	43
169	19	23	29	43	73	242	254	151	39	88	18	127	73	213	141	33	43
170	19	23	29	43	74	243	255	152	40	89	19	128	74	213	141	33	43
171	19	23	29	43	75	244	256	153	41	90	20	129	75	213	141	33	43
172	19	23	29	43	76	245	0	154	42	91	21	130	76	213	141	33	43

Muhammad Izham Bin Norhamadi
B032020039 S2G1

173	19	23	29	43	77	246	1	155	43	92	22	131	77	213	141	33	43
174	19	23	29	43	78	247	2	156	44	93	23	132	78	213	141	33	43
175	19	23	29	43	79	248	3	157	45	94	24	133	79	213	141	33	43
176	19	23	29	43	80	249	4	158	46	95	25	134	80	213	141	33	43
177	19	23	29	43	81	250	5	159	47	96	26	135	81	213	141	33	43
178	19	23	29	43	82	251	6	160	48	97	27	136	82	213	141	33	43
179	19	23	29	43	83	252	7	161	49	98	28	137	83	213	141	33	43
180	19	23	29	43	84	253	8	162	50	99	29	138	84	213	141	33	43
181	19	23	29	43	85	254	9	163	51	100	30	139	85	213	141	33	43
182	19	23	29	43	86	255	10	164	52	101	31	140	86	213	141	33	43
183	19	23	29	43	87	256	11	165	53	102	32	141	87	213	141	33	43
184	19	23	29	43	88	0	12	166	54	103	33	142	88	213	141	33	43
185	19	23	29	43	89	1	13	167	55	104	34	143	89	213	141	33	43
186	19	23	29	43	90	2	14	168	56	105	35	144	90	213	141	33	43
187	19	23	29	43	91	3	15	169	57	106	36	145	91	213	141	33	43
188	19	23	29	43	92	4	16	170	58	107	37	146	92	213	141	33	43
189	19	23	29	43	93	5	17	171	59	108	38	147	93	213	141	33	43
190	19	23	29	43	94	6	18	172	60	109	39	148	94	213	141	33	43
191	19	23	29	43	95	7	19	173	61	110	40	149	95	213	141	33	43
192	19	23	29	43	96	8	20	174	62	111	41	150	96	213	141	33	43
193	19	23	29	43	97	9	21	175	63	112	42	151	97	213	141	33	43
194	19	23	29	43	98	10	22	176	64	113	43	152	98	213	141	33	43
195	19	23	29	43	99	11	23	177	65	114	44	153	99	213	141	33	43
196	19	23	29	43	100	12	24	178	66	115	45	154	100	213	141	33	43
197	19	23	29	43	101	13	25	179	67	116	46	155	101	213	141	33	43
198	19	23	29	43	102	14	26	180	68	117	47	156	102	213	141	33	43
199	19	23	29	43	103	15	27	181	69	118	48	157	103	213	141	33	43
200	19	23	29	43	104	16	28	182	70	119	49	158	104	213	141	33	43