Bài kiểm tra 1 giữa kì – Nhập môn An toàn thông tin

Họ và tên: Lê Minh Bình

MSSV: 18020214

1. Xây dựng đường cong Elliptic với p=127 và p=827 với số điểm là số nguyên tố, mỗi sv có một bộ giá trị (a, b) khác nhau. Lập bảng kP với P là điểm thuộc đường cong và k chạy từ 1 đến cấp của đường cong.

a. $p = 127, a = 10, b = 9$

Phương trình: $y^2 = x^3 + 10x + 9 \; mod \; 127$

Số điểm: 141 (bao gồm điểm vô cực)

Điểm sinh: $P = (0,3)$

Bảng giá trị kP:

kP	1	2	3	4	5	6	7	8	9	10
Điểm	(0,3)	(31,3)	(122,71)	(2,75)	(24,22)	(28,123)	(107,119)	(13,47)	(21,92)	(20,9)
kP	11	12	13	14	15	16	17	18	19	20
Điểm	(22,92)	(66,111)	(7,101)	(62,18)	(38,123)	(36,17)	(79,58)	(82,1)	(117,68)	(84,35)
kP	21	22	23	24	25	26	27	28	29	30
Điểm	(61,4)	(56,121)	(108,96)	(12,29)	(95,24)	(103,13)	(18,68)	(124,29)	(64,86)	(60,7)
kP	31	32	33	34	35	36	37	38	39	40
Điểm	(68,65)	(45,12)	(16,7)	(6,83)	(73,82)	(25,3)	(102,124)	(123,64)	(54,122)	(111,84)
kP	41	42	43	44	45	46	47	48	49	50
Điểm	(58,116)	(23,77)	(14,9)	(46,74)	(76,84)	(119,59)	(57,15)	(120,72)	(29,47)	(100,73)
kP	51	52	53	54	55	56	57	58	59	60
Điểm	(44,17)	(118,98)	(53,119)	(99,111)	(4,85)	(67,84)	(85,8)	(63,49)	(19,94)	(94,8)
kP	61	62	63	64	65	66	67	68	69	70
Điểm	(49,66)	(33,9)	(51,57)	(78,19)	(70,38)	(89,16)	(47,11)	(88,102)	(74,9)	(30,125)
kP	71	72	73	74	75	76	77	78	79	80
Điểm	(30,2)	(74,118)	(88,25)	(47,17)	(89,111)	(70,89)	(78,108)	(51,7)	(33,118)	(49,61)

kP	81	82	83	84	85	86	87	88	89	90
Điểm	(94,119)	(19,33)	(63,78)	(85,47)	(67,43)	(4,42)	(99,16)	(53,8)	(118,29)	(44,11)
kP	91	92	93	94	95	96	97	98	99	100
Điểm	(100,54)	(29,8)	(120,55)	(57,112)	(119,68)	(76,43)	(46,53)	(14,37)	(23,5)	(58,11)
kP	101	102	103	104	105	106	107	108	109	110
Điểm	(111,43)	(54,5)	(123,63)	(102,3)	(25,124)	(73,45)	(6,44)	(16,57)	(45,115)	(68,62)
kP	111	112	113	114	115	116	117	118	119	120
Điểm	(60,57)	(64,41)	(124,98)	(18,59)	(103,114)	(95,103)	(12,98)	(108,31)	(56,6)	(61,123)
kP	121	122	123	124	125	126	127	128	129	130
Điểm	(84,92)	(117,59)	(82,126)	(79,69)	(36,11)	(38,4)	(62,109)	(7,26)	(66,16)	(22,35)
kP	131	132	133	134	135	136	137	138	139	140
Điểm	(20,118)	(21,35)	(13,8)	(107,8)	(28,4)	(24,105)	(2,52)	(122,56)	(31,97)	(0,124)

b. $p = 827, a = 10, b = 9$

Phương trình: $y^2 = x^3 + 10x + 9 \; mod \; 827$

Số điểm: 882 (bao gồm điểm vô cực)

Điểm sinh: $P = (8{,}684)$

Bảng giá trị kP:

kP	1	2	3	4	5	6	7	8	9	10
Điểm	(8,684)	(367,38)	(486,6)	(506,58)	(476,719)	(18,478)	(663,404)	(478,628)	(121,255)	(288,218)
kP	11	12	13	14	15	16	17	18	19	20
Điểm	(82,467)	(251,755)	(496,191)	(455,62)	(728,457)	(666,146)	(321,414)	(155,69)	(87,406)	(398,657)
kP	21	22	23	24	25	26	27	28	29	30
Điểm	(690,292)	(138,533)	(278,393)	(617,441)	(437,139)	(460,563)	(352,279)	(173,657)	(447,696)	(46,417)
kP	31	32	33	34	35	36	37	38	39	40
Điểm	(658,401)	(546,82)	(774,17)	(119,163)	(176,261)	(638,282)	(134,58)	(598,462)	(621,825)	(472,7)
kP	41	42	43	44	45	46	47	48	49	50
Điểm	(826,705)	(366,427)	(222,61)	(74,111)	(412,568)	(4,453)	(687,42)	(256,17)	(821,154)	(351,39)
kP	51	52	53	54	55	56	57	58	59	60
Điểm	(570,34)	(593,799)	(799,659)	(672,417)	(377,51)	(404,76)	(523,9)	(492,303)	(29,626)	(777,416)

kP	61	62	63	64	65	66	67	68	69	70
Điểm	(25,15)	(596,711)	(535,815)	(644,123)	(11,368)	(417,496)	(718,69)	(811,46)	(187,402)	(725,635)
kP	71	72	73	74	75	76	77	78	79	80
Điểm	(623,57)	(12,256)	(678,711)	(645,163)	(159,569)	(52,297)	(40,65)	(512,265)	(107,181)	(504,7)
kP	81	82	83	84	85	86	87	88	89	90
Điểm	(99,807)	(291,124)	(215,538)	(109,41)	(781,758)	(235,791)	(817,33)	(205,128)	(534,28)	(143,297)
kP	91	92	93	94	95	96	97	98	99	100
Điểm	(732,785)	(219,101)	(425,88)	(615,604)	(375,611)	(773,516)	(111,104)	(191,764)	(676,565)	(454,631)
kP	101	102	103	104	105	106	107	108	109	110
Điểm	(692,406)	(795,1)	(467,803)	(765,8)	(740,706)	(302,568)	(618,18)	(63,664)	(100,402)	(660,92)
kP	111	112	113	114	115	116	117	118	119	120
Điểm	(470,598)	(359,305)	(810,46)	(39,593)	(58,23)	(35,318)	(396,73)	(655,175)	(565,493)	(48,421)
kP	121	122	123	124	125	126	127	128	129	130
Điểm	(118,246)	(213,433)	(469,655)	(533,42)	(393,502)	(409,513)	(224,33)	(185,642)	(181,142)	(597,798)
kP	131	132	133	134	135	136	137	138	139	140
Điểm	(716,86)	(382,272)	(695,33)	(586,19)	(380,116)	(298,817)	(116,641)	(311,792)	(653,257)	(344,627)

kP	141	142	143	144	145	146	147	148	149	150
Điểm	(430,761)	(431,738)	(473,242)	(294,502)	(170,622)	(0,824)	(505,157)	(349,453)	(319,327)	(737,682)
kP	151	152	153	154	155	156	157	158	159	160
Điểm	(113,259)	(668,806)	(21,514)	(372,768)	(36,391)	(729,38)	(340,273)	(558,789)	(105,132)	(800,498)
kP	161	162	163	164	165	166	167	168	169	170
Điểm	(268,179)	(708,612)	(696,606)	(441,257)	(814,701)	(632,53)	(576,368)	(56,193)	(812,304)	(577,774)
kP	171	172	173	174	175	176	177	178	179	180
Điểm	(434,407)	(667,92)	(712,222)	(189,391)	(182,612)	(411,709)	(123,23)	(540,425)	(619,299)	(816,755)
kP	181	182	183	184	185	186	187	188	189	190
Điểm	(33,367)	(309,784)	(521,599)	(342,553)	(24,798)	(807,756)	(103,151)	(756,579)	(199,266)	(80,595)
kP	191	192	193	194	195	196	197	198	199	200
Điểm	(689,399)	(587,72)	(629,598)	(474,374)	(438,713)	(34,799)	(796,729)	(499,137)	(68,193)	(220,279)
kP	201	202	203	204	205	206	207	208	209	210
Điểm	(626,442)	(806,46)	(497,136)	(428,705)	(54,58)	(106,362)	(420,79)	(801,73)	(562,14)	(790,208)
kP	211	212	213	214	215	216	217	218	219	220
Điểm	(156,305)	(146,217)	(339,538)	(792,179)	(423,135)	(378,762)	(516,398)	(115,76)	(172,583)	(282,342)

kP	221	222	223	224	225	226	227	228	229	230
Điểm	(37,312)	(270,481)	(502,45)	(599,51)	(605,663)	(405,398)	(255,548)	(383,768)	(803,825)	(776,219)
kP	231	232	233	234	235	236	237	238	239	240
Điểm	(528,432)	(240,459)	(234,683)	(656,8)	(221,51)	(337,47)	(384,742)	(595,268)	(363,79)	(254,504)
kP	241	242	243	244	245	246	247	248	249	250
Điểm	(47,817)	(639,769)	(688,286)	(568,714)	(400,122)	(566,597)	(169,466)	(200,28)	(154,504)	(144,322)
kP	251	252	253	254	255	256	257	258	259	260
Điểm	(145,82)	(798,77)	(388,592)	(550,74)	(241,805)	(449,95)	(373,668)	(110,655)	(361,592)	(735,794)
kP	261	262	263	264	265	266	267	268	269	270
Điểm	(722,763)	(280,743)	(381,807)	(285,96)	(670,154)	(53,224)	(360,617)	(230,2)	(140,325)	(343,83)
kP	271	272	273	274	275	276	277	278	279	280
Điểm	(296,477)	(702,28)	(290,45)	(70,653)	(129,617)	(324,441)	(125,513)	(197,292)	(590,615)	(79,96)
kP	281	282	283	284	285	286	287	288	289	290
Điểm	(322,542)	(327,735)	(495,734)	(402,55)	(295,767)	(813,596)	(22,87)	(88,719)	(308,632)	(41,678)
kP	291	292	293	294	295	296	297	298	299	300
Điểm	(614,178)	(646,804)	(263,108)	(91,204)	(336,625)	(273,289)	(739,39)	(28,702)	(767,535)	(713,386)

kP	301	302	303	304	305	306	307	308	309	310
Điểm	(362,268)	(514,775)	(560,57)	(555,229)	(538,729)	(259,582)	(208,59)	(738,238)	(93,25)	(202,499)
kP	311	312	313	314	315	316	317	318	319	320
Điểm	(494,291)	(559,318)	(98,563)	(163,673)	(206,29)	(647,39)	(793,683)	(229,63)	(444,62)	(223,387)
kP	321	322	323	324	325	326	327	328	329	330
Điểm	(238,153)	(51,138)	(312,522)	(683,62)	(457,754)	(809,567)	(237,353)	(751,408)	(602,436)	(422,792)
kP	331	332	333	334	335	336	337	338	339	340
Điểm	(741,599)	(627,683)	(755,207)	(768,16)	(23,1)	(822,764)	(764,215)	(463,96)	(269,264)	(338,617)
kP	341	342	343	344	345	346	347	348	349	350
Điểm	(724,549)	(262,147)	(697,268)	(347,2)	(753,119)	(89,543)	(564,437)	(394,371)	(592,518)	(310,665)
kP	351	352	353	354	355	356	357	358	359	360
Điểm	(196,823)	(271,56)	(527,416)	(519,375)	(698,803)	(731,439)	(757,12)	(403,404)	(723,43)	(459,405)
kP	361	362	363	364	365	366	367	368	369	370
Điểm	(418,547)	(26,738)	(802,242)	(245,427)	(588,423)	(225,282)	(703,634)	(392,599)	(704,142)	(78,592)
kP	371	372	373	374	375	376	377	378	379	380
Điểm	(231,696)	(779,706)	(518,48)	(166,593)	(594,648)	(379,242)	(482,1)	(370,738)	(693,516)	(320,729)

kP	381	382	383	384	385	386	387	388	389	390
Điểm	(248,172)	(72,59)	(761,635)	(769,142)	(788,128)	(62,296)	(643,785)	(498,306)	(354,15)	(71,637)
kP	391	392	393	394	395	396	397	398	399	400
Điểm	(650,11)	(14,558)	(419,504)	(622,593)	(147,534)	(747,643)	(171,302)	(368,733)	(524,376)	(149,131)
kP	401	402	403	404	405	406	407	408	409	410
Điểm	(38,507)	(791,545)	(293,314)	(279,785)	(135,706)	(216,4)	(188,516)	(823,628)	(661,128)	(10,783)
kP	411	412	413	414	415	416	417	418	419	420
Điểm	(158,161)	(742,133)	(350,411)	(94,792)	(600,15)	(353,199)	(736,687)	(446,457)	(567,816)	(192,283)
kP	421	422	423	424	425	426	427	428	429	430
Điểm	(328,337)	(700,759)	(7,51)	(489,803)	(770,472)	(530,438)	(112,173)	(233,509)	(168,635)	(452,341)
kP	431	432	433	434	435	436	437	438	439	440
Điểm	(301,591)	(448,15)	(480,37)	(641,63)	(819,288)	(44,79)	(9,826)	(299,171)	(733,398)	(346,152)
kP	441	442	443	444	445	446	447	448	449	450
Điểm	(797,0)	(346,675)	(733,429)	(299,656)	(9,1)	(44,748)	(819,539)	(641,764)	(480,457)	(448,677)
kP	451	452	453	454	455	456	457	458	459	460
Điểm	(301,236)	(452,486)	(168,192)	(233,318)	(112,654)	(530,389)	(770,355)	(489,24)	(7,317)	(700,68)

kP	461	462	463	464	465	466	467	468	469	470
Điểm	(328,49)	(192,544)	(567,11)	(446,37)	(736,14)	(353,628)	(600,812)	(94,35)	(350,416)	(742,694)
kP	471	472	473	474	475	476	477	478	479	480
Điểm	(158,666)	(10,44)	(661,699)	(823,199)	(188,311)	(216,427)	(135,121)	(279,42)	(293,513)	(791,282)
kP	481	482	483	484	485	486	487	488	489	490
Điểm	(38,32)	(149,696)	(524,451)	(368,94)	(171,525)	(747,184)	(147,293)	(622,234)	(419,323)	(14,269)
kP	491	492	493	494	495	496	497	498	499	500
Điểm	(650,717)	(71,19)	(354,677)	(498,521)	(643,42)	(62,531)	(788,699)	(769,685)	(761,192)	(72,768)
kP	501	502	503	504	505	506	507	508	509	510
Điểm	(248,655)	(320,98)	(693,311)	(370,89)	(482,817)	(379,585)	(594,179)	(166,234)	(518,779)	(779,121)
kP	511	512	513	514	515	516	517	518	519	520
Điểm	(231,131)	(78,235)	(704,685)	(392,228)	(703,193)	(225,545)	(588,404)	(245,4)	(802,585)	(26,89)
kP	521	522	523	524	525	526	527	528	529	530
Điểm	(418,28)	(459,422)	(723,397)	(403,423)	(757,707)	(731,388)	(698,24)	(519,452)	(527,411)	(271,267)
kP	531	532	533	534	535	536	537	538	539	540
Điểm	(196,4)	(310,162)	(592,309)	(394,456)	(564,39)	(89,284)	(753,708)	(347,807)	(697,559)	(262,68)

kP	541	542	543	544	545	546	547	548	549	550
Điểm	(724,278)	(338,21)	(269,563)	(463,731)	(764,612)	(822,63)	(23,826)	(768,667)	(755,62)	(627,144)
kP	551	552	553	554	555	556	557	558	559	560
Điểm	(741,228)	(422,35)	(602,391)	(751,419)	(237,474)	(809,26)	(457,73)	(683,765)	(312,305)	(51,689)
kP	561	562	563	564	565	566	567	568	569	570
Điểm	(238,674)	(223,44)	(444,207)	(229,197)	(793,144)	(647,788)	(206,798)	(163,154)	(98,264)	(559,509)
kP	571	572	573	574	575	576	577	578	579	580
Điểm	(494,536)	(202,328)	(93,802)	(738,589)	(208,237)	(259,245)	(538,98)	(555,598)	(560,257)	(514,52)
kP	581	582	583	584	585	586	587	588	589	590
Điểm	(362,559)	(713,441)	(767,292)	(28,125)	(739,437)	(273,538)	(336,202)	(91,623)	(263,719)	(646,23)
kP	591	592	593	594	595	596	597	598	599	600
Điểm	(614,649)	(41,149)	(308,195)	(88,108)	(22,74)	(813,231)	(295,6)	(402,772)	(495,93)	(327,92)
kP	601	602	603	604	605	606	607	608	609	610
Điểm	(322,285)	(79,731)	(590,212)	(197,535)	(125,314)	(324,386)	(129,21)	(70,174)	(290,782)	(702,547)
kP	611	612	613	614	615	616	617	618	619	620
Điểm	(296,35)	(343,744)	(140,502)	(230,825)	(360,21)	(53,603)	(670,673)	(285,731)	(381,2)	(280,84)

kP	621	622	623	624	625	626	627	628	629	630
Điểm	(722,64)	(735,33)	(361,235)	(110,172)	(373,159)	(449,732)	(241,22)	(550,753)	(388,235)	(798,75)
kP	631	632	633	634	635	636	637	638	639	640
Điểm	(145,745)	(144,505)	(154,323)	(200,799)	(169,361)	(566,23)	(400,705)	(568,113)	(688,541)	(639,58)
kP	641	642	643	644	645	646	647	648	649	650
Điểm	(47,1)	(254,323)	(363,748)	(595,559)	(384,85)	(337,357)	(221,317)	(656,747)	(234,144)	(240,368)
kP	651	652	653	654	655	656	657	658	659	660
Điểm	(528,395)	(776,608)	(803,2)	(383,59)	(255,279)	(405,429)	(605,164)	(599,317)	(502,377)	(270,346)
kP	661	662	663	664	665	666	667	668	669	670
Điểm	(37,515)	(282,485)	(172,244)	(115,67)	(516,429)	(378,65)	(423,692)	(792,648)	(339,289)	(146,61)
kP	671	672	673	674	675	676	677	678	679	680
Điểm	(156,522)	(790,619)	(562,813)	(801,754)	(420,748)	(106,465)	(54,769)	(428,122)	(497,691)	(806,781)
kP	681	682	683	684	685	686	687	688	689	690
Điểm	(626,385)	(220,548)	(68,634)	(499,69)	(796,98)	(34,28)	(438,114)	(474,453)	(629,229)	(587,755)
kP	691	692	693	694	695	696	697	698	699	700
Điểm	(689,428)	(80,232)	(199,561)	(756,248)	(103,676)	(807,71)	(24,29)	(342,274)	(521,228)	(309,43)

kP	701	702	703	704	705	706	707	708	709	710
Điểm	(33,46)	(816,72)	(619,528)	(540,402)	(123,804)	(411,118)	(182,215)	(189,436)	(712,605)	(667,735)
kP	711	712	713	714	715	716	717	718	719	720
Điểm	(434,42)	(577,53)	(812,523)	(56,634)	(576,459)	(632,297)	(814,126)	(441,57)	(696,221)	(708,215)
kP	721	722	723	724	725	726	727	728	729	730
Điểm	(268,648)	(800,329)	(105,695)	(558,38)	(340,554)	(729,789)	(36,436)	(372,59)	(21,313)	(668,21)
kP	731	732	733	734	735	736	737	738	739	740
Điểm	(113,568)	(737,145)	(319,5)	(349,374)	(505,67)	(0,3)	(170,205)	(294,325)	(473,585)	(431,89)
kP	741	742	743	744	745	746	747	748	749	750
Điểm	(430,66)	(344,2)	(653,57)	(311,35)	(116,186)	(298,1)	(380,711)	(586,808)	(695,794)	(382,555)
kP	751	752	753	754	755	756	757	758	759	760
Điểm	(716,741)	(597,29)	(181,685)	(185,185)	(224,794)	(409,314)	(393,325)	(533,407)	(469,172)	(213,394)
kP	761	762	763	764	765	766	767	768	769	770
Điểm	(118,581)	(48,406)	(565,334)	(655,652)	(396,754)	(35,509)	(58,804)	(39,234)	(810,367)	(359,522)
kP	771	772	773	774	775	776	777	778	779	780
Điểm	(470,229)	(660,735)	(100,425)	(63,163)	(618,809)	(302,259)	(740,121)	(765,819)	(467,24)	(795,826)

kP	781	782	783	784	785	786	787	788	789	790
Điểm	(692,421)	(454,196)	(676,262)	(191,63)	(111,723)	(773,311)	(375,216)	(615,223)	(425,739)	(219,726)
kP	791	792	793	794	795	796	797	798	799	800
Điểm	(732,42)	(143,53)	(534,547)	(205,699)	(817,497)	(235,36)	(781,69)	(109,417)	(215,289)	(291,703)
kP	801	802	803	804	805	806	807	808	809	810
Điểm	(99,2)	(504,127)	(107,646)	(512,562)	(40,177)	(52,53)	(159,258)	(645,664)	(678,116)	(12,571)
kP	811	812	813	814	815	816	817	818	819	820
Điểm	(623,77)	(725,192)	(187,425)	(811,367)	(718,758)	(417,331)	(11,459)	(644,704)	(535,12)	(596,116)
kP	821	822	823	824	825	826	827	828	829	830
Điểm	(25,677)	(777,411)	(29,201)	(492,524)	(523,737)	(404,751)	(377,776)	(672,41)	(799,168)	(593,28)
kP	831	832	833	834	835	836	837	838	839	840
Điểm	(570,793)	(351,437)	(821,673)	(256,657)	(687,407)	(4,374)	(412,259)	(74,716)	(222,766)	(366,4)
kP	841	842	843	844	845	846	847	848	849	850
Điểm	(826,122)	(472,757)	(621,2)	(598,365)	(134,769)	(638,545)	(176,566)	(119,664)	(774,81)	(546,7)
kP	851	852	853	854	855	856	857	858	859	860
Điểm	(658,426)	(46,41)	(447,131)	(173,17)	(352,548)	(460,264)	(437,688)	(617,386)	(278,434)	(138,294)

kP	861	862	863	864	865	866	867	868	869	870
Điểm	(690,535)	(398,17)	(87,421)	(155,758)	(321,413)	(666,681)	(728,37)	(455,207)	(496,636)	(251,72)
kP	871	872	873	874	875	876	877	878	879	880
Điểm	(82,36)	(288,609)	(121,572)	(478,199)	(663,423)	(18,349)	(476,108)	(506,247)	(486,227)	(367,789)
kP	881									
Điểm	(8,143)									

2. Mã hóa và giải mã bằng 2 hệ mật đã học với điểm M có hoành độ được nhúng bởi x=Chữ cái mà bạn cho là ý nghĩa đối với bạn, khi p=127, và x= Bộ hai chữ cái mà bạn coi là ý nghĩa với p=827.

2.1. Hệ mật EC – ElGamal

a. $p = 127, a = 10, b = 9, x = 20(U)$

**** Mã hóa***

Đường cong: $y^2 = x^3 + 10x + 9 \; mod \; 127$

Tập điểm: $E_p(a, b) = E_{127}(10,9)$

Điểm sinh: $G = (0,3)$

Tin nhắn $x = 20$ (U) được mã hóa bởi điểm $P_M = (20,118) \in E_{127}(10,9)$

Với khóa bí mật $n_B = 19$ khóa công khai là $P_B = n_B G = 19(0,3) = (117,68)$

Chọn số ngẫu nhiên $k = 38$, khóa công khai $P_B = (117,68)$ mã hóa thành cặp điểm

$$P_c = [(kG), (P_M + kP_B)] = \big[(123,64), \big((20,118) + 38(117,68)\big)\big] = [(123,64), (100,54)]$$

**** Giải mã***

$$(P_M + kP_B) - [n_B(kG)] = (100,54) - [19(123,64)] = (100,54) - (99,16) = (100,54) + (99,111) = (20,118) = P_M$$

b. $p = 127, a = 10, b = 9, x = 44(CC)$

**** Mã hóa***

Đường cong: $y^2 = x^3 + 10x + 9 \; mod \; 827$

Tập điểm: $E_p(a,b) = E_{827}(10,9)$

Điểm sinh: $G = (8,684)$

Tin nhắn $x = 44$ (CC) được mã hóa bởi điểm $P_M = (44,79) \in E_{827}(10,9)$

Với khóa bí mật $n_B = 19$ khóa công khai là $P_B = n_B G = 19(8,684) = (87,406)$

Chọn số ngẫu nhiên $k = 38$, khóa công khai $P_B = (87,406)$ mã hóa thành cặp điểm

$$P_c = [(kG), (P_M + kP_B)] = \big[(598,462), \big((44,79) + 38(87,406)\big)\big] = [(598,462), (741,599)]$$

**** Giải mã***

$$(P_M + kP_B) - [n_B(kG)] = (741,599) - [19(598,462)] = (741,59) - (800,329) = (44,79) = P_M$$

2.2. Hệ mật Massey – Omura

a. $p = 127, a = 10, b = 9, x = 20(U)$

**** Mã hóa***

Đường cong: $y^2 = x^3 + 10x + 9 \; mod \; 127$

$N = 141$

Tin nhắn $x = 20$ (U) được nhúng bởi điểm $M = (20,118) \in E_{127}(10,9)$

Người gửi chọn số bí mật $m_A = 5$ thỏa mãn $(m_A, N) = 1$

Người nhận chọn số bí mật $m_B = 7$ thỏa mãn $(m_B, N) = 1$

Người gửi tính $M_1 = m_A M = 5(20,118) = (84,35)$ rồi gửi cho người nhận.

Người nhận tính $M_2 = m_B M_1 = 7(124,29) = (7,101)$ rồi gửi cho người gửi.

Người gửi tính $M_3 = m_A^{-1} M_2 = 51(70,38) = (124,29)$ rồi gửi cho người nhận.

**** Giải mã***

Người nhận tính $M_4 = m_b^{-1} M_3 = 109(7,101) = (20,118) = M$

b. $p = 827, a = 10, b = 9, x = 44(CC)$

**** Mã hóa***

Đường cong: $y^2 = x^3 + 10x + 9 \; mod \; 827$

$N = 882$

Tin nhắn $x = 44$ (CC) được nhúng bởi điểm $M = (44,79) \in E_{82} \; (10,9)$

Người gửi chọn số bí mật $m_A = 29$ thỏa mãn $(m_A, N) = 1$

Người nhận chọn số bí mật $m_B = 31$ thỏa mãn $(m_B, N) = 1$

Người gửi tính $M_1 = m_A M = 29(44,79) = (363,79)$ rồi gửi cho người nhận.

Người nhận tính $M_2 = m_B M_1 = 31(363,79) = (534,547)$ rồi gửi cho người gửi.

Người gửi tính $M_3 = m_A^{-1} M_2 = 770(70,38) = (402,55)$ rồi gửi cho người nhận.

**** Giải mã***

Người nhận tính $M_4 = m_b^{-1} M_3 = 747(7,101) = (44,79) = M$

3) Xây dựng chữ ký và kiểm thử theo các sơ đồ chữ ký trên đường cong Elliptic với x như trong phần 2.

3.1. ECDSA

a. $p = 127, a = 10, b = 9, x = 20(U)$

**** Xây dựng chữ kí***

Đường cong: $y^2 = x^3 + 10x + 9\ mod\ 127$

$N\ =\ 141$

$G(0,3)$

Tạo cặp khóa:

- Chọn số ngẫu nhiên $d = 19$ làm khóa riêng, khi đó $Q = dG = (117,68)$
- Khóa công khai của người gửi là tổ hợp $(E_{127}(10,9), (0,3), 141, (117,68))$

Tạo chữ kí

- Chọn số ngẫu nhiên $k = 46$, tính được $kG = 46(0,3) = (119,59)$
- $r = x_1\ mod\ N = 119\ mod\ 141 = 119$
- $h = H(M) =$

$$1143184334757257700049096573617336324472646451371792795805256478773538333667618933592499747583897482534771189285304268237339453992204267557666299961292837 9$$

- $s = (h + d * r) * k^{-1}\ mod\ N = 5$

Khi đó chữ kí của người gửi trên bản tin M là $(119,5)$

**** Kiểm thử***

Người nhận nhận được chữ kí trên khóa công khai $(E_{127}(10,9),(0,3),141,(117,68)).\backslash$

Các giá trị r, s đều nằm trong khoảng $[1, N-1]$.

$w = s^{-1}\ mod\ N = 113$

$h = H(M)$

$= 114318433475725770004909657361733632447264645137179279580525647877353833366761893$
$35924997475838974825347711892853042682373394539922042675576662999612928379$

$(h * w\ mod\ N) * G + (r * w\ mod\ N) * Q = (76,84) + (0,3) = (119,59)$

$v = x_0\ mod\ N = 119 = r$

Chữ kí được xác minh.

b. $p = 827, a = 10, b = 9, x = 44(CC)$

**** Xây dựng chữ kí***

Đường cong: $y^2 = x^3 + 10x + 9\ mod\ 827$

$N\ =\ 882$

$G(8,684)$

Tạo cặp khóa:

- Chọn số ngẫu nhiên $d = 19$ làm khóa riêng, khi đó $Q = dG = (87,406)$
- Khóa công khai của người gửi là tổ hợp $(E_{827}(10,9),(8,684),882,(87,406))$

Tạo chữ kí

- Chọn số ngẫu nhiên $k = 17$, tính được $kG = 17(8,684) = (321,414)$

- $r = x_1 \ mod \ N = 321 \ mod \ 882 = 321$

- $h = H(M) =$

$$7185609867299172400579209950287802822100567696006579099549561059130877069607508060919$$
$$32284628940820546404742063513857928380985920916910813177046995048087 8$$

- $s = (h + d * r) * k^{-1} \ mod \ N = 379$

Khi đó chữ kí của người gửi trên bản tin M là $(321,379)$

**** Kiểm thử***

Người nhận nhận được chữ kí trên khóa công khai $(E_{82} \ (10,9), (8,684), 882, (55,795))$.\

Các giá trị r, s đều nằm trong khoảng $[1, N - 1]$.

$w = s^{-1} \ mod \ N = 505$

$h = H(M)$

$$= 7185609867299172400579209950287802822100567696006579099549561059130877069607508060919$$
$$32284628940820546404742063513857928380985920916910813177046995048087 8$$

$(h * w \ mod \ N) * G + (r * w \ mod \ N) * Q = (119,664) + (570,34) = (321,414)$

$v = x_0 \ mod \ N = 321 = r$

Chữ kí được xác minh.

3.2. ECGDSA

$a.\ p = 127, a = 10, b = 9, x = 20(U)$

**** Xây dựng chữ kí***

Đường cong: $y^2 = x^3 + 10x + 9\ mod\ 127$

$N\ =\ 141$

$G(0,3)$

Tạo cặp khóa:

- Chọn số ngẫu nhiên $d = 19$ làm khóa riêng, khi đó $Q = (d^{-1}\ mod\ N)\ G = (118,98)$
- Khóa công khai của người gửi là tổ hợp $(E_{127}(10,9), (0,3), 141, (118,98))$

Tạo chữ kí

- Chọn số ngẫu nhiên $k = 46$, tính được $kG = 46(0,3) = (119,59)$
- $r = x_1\ mod\ N = 119\ mod\ 141 = 119$
- $h = H(M) =$

$$1143184334757257700049096573617336324472646451371792795805256478773538333667618933592499747583897482534771189285304268237339453992204267557666299961292837 9$$

- $s = (k * r - h) * d\ mod\ N = 44$

Khi đó chữ kí của người gửi trên bản tin M là $(119,44)$

**** Kiểm thử***

Người nhận nhận được chữ kí trên khóa công khai $(E_{127}(10,9), (0,3), 141, (117,68))$.\

Các giá trị r, s đều nằm trong khoảng $[1, N-1]$.

$w = r^{-1}\ mod\ N = 32$

$h = H(M)$

$= 114318433475725770004909657361733632447264645137179279580525647877353833366761893$

$359249974758389748253477118928530426823733945399220426755766629996129283 79$

$(h * w\ mod\ N) * G + (s * w\ mod\ N) * Q = (102,124) + (21,92) = (119,59)$

$v = x_0\ mod\ N = 119 = r$

Chữ kí được xác minh.

b. $p = 827, a = 10, b = 9, x = 44(CC)$

**** Xây dựng chữ kí***

Đường cong: $y^2 = x^3 + 10x + 9\ mod\ 827$

$N\ =\ 882$

$G(0,3)$

Tạo cặp khóa:

- Chọn số ngẫu nhiên $d = 19$ làm khóa riêng, khi đó $Q = (d^{-1}\ mod\ N)\ G = (457,754)$
- Khóa công khai của người gửi là tổ hợp $(E_{827}(10,9), (8,684), 882, (457,754))$

Tạo chữ kí

- Chọn số ngẫu nhiên $k = 2$, tính được $kG = 2(8,684) = (367,38)$

- $r = x_1 \ mod \ N = 367 \ mod \ 882 = 367$

- $h = H(M) =$

$$718560986729917240057920995028780282210056769600657909954956105913087706960750806091932284628940820546404742063513857928380985920916910813177046995048087 8$$

- $s = (k * r - h) * d \ mod \ N = 612$

Khi đó chữ kí của người gửi trên bản tin M là $(367,612)$

**** Kiểm thử***

Người nhận nhận được chữ kí trên khóa công khai $(E_{827}(10,9), (8,684), 882, (457,754))$.\

Các giá trị r, s đều nằm trong khoảng $[1, N-1]$.

$w = r^{-1} \ mod \ N = 733$

$h = H(M)$

$$= 718560986729917240057920995028780282210056769600657909954956105913087706960750806091932284628940820546404742063513857928380985920916910813177046995048087 8$$

$(h * w \ mod \ N) * G + (s * w \ mod \ N) * Q = (347,2) + (155,758) = (457,754)$

$v = x_0 \ mod \ N = 457 = r$

Chữ kí được xác minh.