Національний Технічний Університет України
“Київський Політехнічний Інститут”
Фізико-Технічний Інститут

ГЕШ-ФУНКЦІЇ ТА КОДИ АВТЕНТИЧНОСТІ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1:
Побудова атак на геш-функції
Варіант 9

Виконала студентка 4-го курсу
групи ФІ-14
Недашківська Аріна

Київ 2024

1 Мета роботи

Дослідити криптографічні властивості геш-функцій, засвоїти еталонні оцінки стійкості геш-функцій, перевірити на практиці теоретичні положення.

2 Теоретичні відомості

2.1 Випадковий пошук прообразу

Випадковий пошук прообразу - атака загального виду на геш-функцію, метою якого є знайти прообраз для фіксованого геш значення або другий прообраз для фіксованого повідомлення, шляхом випадкового вибору без повернень повідомлень і обчислення їх значень. В цьому комп'ютерному практикумі ми розглядали другий варіант - ми фіксували повідомлення і шукали до нього другий прообраз, змінюючи саме повідомлення.

Успіх атаки оцінюється таким чином:

$$Pr(\text{успіху}) \geq 1 - e^{-\frac{r}{2^n}}$$

де r - кількість ітерацій, яку здійснила атака; n - розмір вихідного гешу

Очікувана складність атаки $O(2^n)$ викликів геш-функції. Для цього варіанту це $O(2^{16})$ викликів геш функції.

2.2 Атака "днів народжень"

Атака днів народжень - атака загального виду на геш-функцію, метою якого є знайти колізію. Протягом атаки ми зберігаємо усі повідомлення і їх геші, які розглянули - і при генерації нового повідомлення співставляємо його геш зі збереженими гешами. Якщо співпадає - маємо колізію, якщо ні - зберігаємо повідомлення і геш та генеруємо нове.

Успіх атаки оцінюється таким чином:

$$Pr(\text{успіху}) \geq 1 - e^{-\frac{r^2}{2 \cdot 2^n}}$$

де r - кількість ітерацій, яку здійснила атака; n - розмір вихідного гешу.

Очікувана складність атаки $O(2^{n/2})$ викликів геш-функції. Для цього варіанту це $O(2^{n/2}) = O(2^{16})$ викликів геш функціїі(як і в атаці пошуку прообразу виходить).

3 Хід роботи

Згідно варіанту, розглядалась геш-функція RIPEMD-320. Сформовані повідомлення, які містять повне ПІБ, для кожного варіанту атаки генерувались випадковим чином за такою схемою:

NedashkivskaArinaVitalyivna****

де * - від 0 до 9 випадкових чисел.

3.1 Випадковий пошук прообразу

3.1.1 Перший варіант атаки

Сформоване повідомлення: NedashkivskaArinaVitalyivna2901
Зафіксоване геш значення:
ed86cae96a215947a8a23cf59c0f47123a670d795cd3317d9af428fd756e7c58c9aa3eb270fb9303

Перші 30 повідомлень та їх геші:

Повідомлення	Геш-значення
NedashkivskaArinaVitalyivna29011	01277bac9b87830d4b8e03d1a5df699953d0334169eda6779b4345397422a4f8f454eff1176b2042
NedashkivskaArinaVitalyivna29012	c5ebd1eb515c84b89964be16216e4bf938441e3a134eb57e055baaa04e790d5a78e8d4970175 3ab4
NedashkivskaArinaVitalyivna29013	216bc9518df93ec0aeafc15f04bda809590ceb4f5435b9d5bdfd096839ad29e19c5a069dbb97e6cf
NedashkivskaArinaVitalyivna29014	3521cdc3a7b01e1f71de7cf11e568c12ec0e4d67aa14dc3ecae12347c61b14bfffa741a10cf2301b
NedashkivskaArinaVitalyivna29015	de2e7285203ea320db1cab23e17d43e519f5013dd2a3fa47936ab01c57b094a5986a949d37ad54b4
NedashkivskaArinaVitalyivna29016	1cf30c975ba2374469fbb0484acc4cc2a5a9b4a0952ff8f1693586116e9f8aca04689e012d619b53
NedashkivskaArinaVitalyivna29017	5805760574618d78371b6054810bbd4ba9b84ef1a17a9f78832c418dbebd9b41c26ce2818fb61911
NedashkivskaArinaVitalyivna29018	9a5553da3fa348d0f223c8e06d355b0ba55b6b71667de95104b3828d9beffa1e8d054b691d7d2299
NedashkivskaArinaVitalyivna29019	85acacc5ca515a043fb07dee14200391fe7c24e5cc12478e28d6915ed45b3fe3312315a4c7359619
NedashkivskaArinaVitalyivna290110	1b913cd228c9aa2f344b3aa9a46ceaf36d7dde8c2c5fc1601e1b42037a2098647fc1ab542bbd18db
NedashkivskaArinaVitalyivna290111	531a6d9869e6ce4ce2edb7bd2f0f9a34ef21d95b29f7c226d497c5bf0f8aed5a707bad842be08923
NedashkivskaArinaVitalyivna290112	146beb90137b0bbc50c64c37a12759c49b9dd79f7de3cb3e647f57b3fd315b5ea2071c44d8ba5125
NedashkivskaArinaVitalyivna290113	e2bf8f7c35dbff2c7779aefdf34d85e9734a3b0509d1d8c3be3b860fc50d3b1e1d6811633906be5f
NedashkivskaArinaVitalyivna290114	6e780cc740e6b5b6952a0db600addf9ff69e66541ac05ba4c213df65c4edb54d2f4c0d2692b64c6b
NedashkivskaArinaVitalyivna290115	ebae4243e6326f26d5312fd4e06f1b97f5d44060abcad18c2233f8bf122720fdf5c3d0152231 3a68
NedashkivskaArinaVitalyivna290116	fdfcd3f344037f3a0b56dccdf502511df266c866d1bd2ccd4fbe561737134248323ded158f55c644
NedashkivskaArinaVitalyivna290117	b7187ed77300ea765391822983c11a503d5a54a0fed0ddb75f80b11ba044a96a85a257558515bfa6
NedashkivskaArinaVitalyivna290118	c9835970204bb73b9396c0f6218c880ec24ed8e476fc6620e45aea3d77350d046304c3a14e853edd
NedashkivskaArinaVitalyivna290119	256fd106a2466689908f2a66e019e20916a19f3cecad2e75c71fd1147839c614b11f8d1c30044db0
NedashkivskaArinaVitalyivna290120	e7973ff4d3d9407d4779d8f2960721a9809c68e05069b927f40fcc961b365acf27cad1fee5e87236
NedashkivskaArinaVitalyivna290121	cba1da6a1ba385d7eb9949645e1c95ab4bb28f4bc9f10745a8bcb80f02197e36bca97b9f00cbc084
NedashkivskaArinaVitalyivna290122	e3f07c59300de8138d90457d0c28ec21b658254f9fc99f9bdbe63cfe53599cbcfb054568f24df5e0
NedashkivskaArinaVitalyivna290123	974748c6d0362200a316f343bd7a26d02179308f45ff93e1e418f0a4efc177eefba658cbc86974fd
NedashkivskaArinaVitalyivna290124	3d1ba4cdfe5a5a804263b72c0a986371266041cd4a05a135c22af4924ed604ecbca711f6010c2237
NedashkivskaArinaVitalyivna290125	d2b37e2b5b8407768a85af4e4be2393ee11d84b7bab63a79534a786410b8c5fcf11f2d3a51d908f5
NedashkivskaArinaVitalyivna290126	2a6838d1558013195a14eef706f4d68b7758542ba4bb14a835fc46a32c3e03e07ceb59bbcfdca895
NedashkivskaArinaVitalyivna290127	1b2523bace7af0cb5f23ff70fca325aff8814afa7eb8809f6f2557e2bc5e63463fb32ad48254c624
NedashkivskaArinaVitalyivna290128	ba148b90aa6846740fc176da9cac1b4a820118216a96b019cbd9d967cd1ea7ed0aa2de3cb3b40a22
NedashkivskaArinaVitalyivna290129	113bd3cc22f01507e4f367514cca14db81141a422d88e741d0727ba4136bf184981d4b5136d22280
NedashkivskaArinaVitalyivna290130	510ebdb98cff339a9866950adcf76406567390117b056dcc04f0dd02d02d80e922a130f62b198a04

Знайшли прообраз для повідомлення за 19617 ітерацій:

NedashkivskaArinaVitalyivna290119617	334b542accfc09d3930b484393078c6e4109debda58fcf49acfe81f231912ca272ca5db3ba8a9303

3.1.2 Другий варіант атаки

Сформоване повідомлення: NedashkivskaArinaVitalyivna8839
Зафіксоване геш значення:
58fcb0583c8322bdc3680260eb1c42329591340871496ce4924ff1b8cf83278bd491b93268100e24

Перші 30 повідомлень та їх геші:

Повідомлення	Геш-значення
NedashkivskaArinaVitalyivWa8839	8d6cfbb0fa3b93126a622567de9c27cca8d9a159a3ad1a0851a10485d5b25aeaa3561d2dbdeb0b25
NedashkivskaArinaVita5yivWa8839	43e2749bcd574c74e4833e72d34b08cdca6b8f43caa09682e5d410ab19975e6948bdfa8d9f4db8d4
Nedashkivsk(ArinaVita5yivWa8839	4ad382e69088937cfe4b8b25fff5360389e9da1403ecc35ba7658f4135ed588e1b1bb9d4cdcab4e9
Nedashkivsk(ArinaVita5yiv<a8839	d8855c6f7cf1a5d222ed281abed9e0654c6f6ed31911a1be9e8beb53987a2c67d44287d4ed5c90d9
Nedashkivsk(Arina-ita5yiv<a8839	606a11ee36e9b1318bfe89037edb59ab3fa930098bc4669f044770d8dd8b908a16594eb3931711d99
Nedashkivsk(ALina-ita5yiv<a8839	75d346b4d71037ae386fd9fe1770466da9d4cbf98d0abcc88cbfb980923df076e4015cdb3f94cffb
Nedashkivsk(ALina-iHa5yiv<a8839	b6c874f05619d1fe50fe3519a5af6e8d4f9334d605157481f86d23637430c0a3884419db001a6c82
NedashkivAk(ALina-iHa5yiv<a8839	b1b21f0d5f7df4c8caf16e5ce7df30e71e002baae3ce3c9f2f3951c37b036acb72fa9e81a6459d7b
Nedash'ivAk(ALina-iHa5yiv<a8839	a64b8a54cffa24563206f759ac941012dbe1790a6796a62ade68efc7221d1609c3066528625e3292
Nedash'irAk(ALina-iHa5yiv<a8839	2d7c6aec337c4a98454cd7aa915fea43d5893f66b77e890e7b82d455f200355761bf54ec7b940917
Nedash'irAk(ALinaViHa5yiv<a8839	f07b472bbf1d55add47e02bafc23a527eb40e36298de8d2d094d23ecc7791354707ed630790b8347
N"dash'irAk(ALinaViHa5yiv<a8839	58cd8214ac54a2dbaa27e0a67a1a150903cbd86f6674f8ddab0003c17c77b10d44aa19b0f34f72e4
N"dash'irAk(ALinaViHa5yfv<a8839	1f65c76d73a706454ab2370593418c672119c739e0470ff68c800450b6dde4ecf9bc9335a31413f8
N"dash'irAk(ALinaViHa5yf:<a8839	12b23f03b9ff9a036343a42a7326f4d19c752cdfcf0f59a22e41b833c49b1bd8b97ee0652393157e
N"tash'irAk(ALinaViHa5yf:<a8839	3ccd0a798a711e05968fd675c7f95833cf56eaef8e850ddba03233b395cdaa03db6a47d5a50c67f2
N"tash'irAk(ALinaViHa5yf:<a8k39	8ea459244c2d33d8db50da9fd5889af75958cd3369ad6b3a2895c304ca80b796ff8d4c22f0753406
N"tUsh'irAk(ALinaViHa5yf:<a8k39	0708a7413fab5b47e7a52f2da4910ab46fdbbcc883f3b97e99103d33ffd1aa8f2e58478279fe6876
N"tUsh'irAkAALinaViHa5yf:<a8k39	4b952284de450acf4f358f4553504196b5b2fef470f93a56e806c7bc6b972c91b5a6c74b83cb0e83
N"tUsh'irAkAALinaVi:a5yf:<a8k39	ec7a60bd7d9a0dec820931a60814c7267dcbabb681df2e722ca49e6663d71b86d9fb914c23bf89d9
N"tUsh'irAkAALinaVi:a5yf:<a8p39	c54a94139f144c30f109dbba96d8984a67925c503e7713bdb2517f7b9703eeafb46c06fb5a32127d
N"tUsh'irAkAALinaVi:y5yf:<a8p39	e651efb176e7cc4477b8ec545e4cde672e3e5b40474a36149ec8c3b10fc5d06842c01ee33942aa30
N"tUsh'irAkAALi$aVi:y5yf:<a8p39	97d12a2a525324a24f86cf9b4ccf1d6912735a1b6d1d50570d6c58a1e422b1aa590a05a523d6b231
N"tUsh'irAkAALi$aVi:y5yf:#a8p39	da0febb0eb74e1f6b971d2a833863206d73deb0623d835ad6c485ec4198cc15ca1b405d99b9540ff
N"tU9h'irAkAALi$aVi:y5yf:#a8p39	c84ed1df94ed2524d985ee2f36a7fb9c55ee43b7ef41f8a4494938e9cf6a293686e4f1a8d3ef1b7e
N"tw9h'irAkAALi$aVi:y5yf:#a8p39	2d7cdaaddf4cfe4b42a128a417ac18a269a38ef4c3f89e9fddf6d6f2a75cc957aebd87659800acd8
a"tw9h'irAkAALi$aVi:y5yf:#a8p39	339ac95fc50c164dbd1ef2579dc94da3414143f65110bc137a738b67ef4f87d15086dd41e77012e3
a"tw9h'irAkAALi$aVi:}5yf:#a8p39	de451ddf7fd995a7238ae82404cd1417c0326e361babc86828901df4e1e03bec8233a33eac0dd4b5
a"tw9h'irAkAALi$aVi:w5yf:#a8p39	dea5b168a83f31112cfc17d5db1ec83cc1c34e27bf0e48858beb3c4dcf8117fc8aa2b095116f99a5
a"twih'irAkAALi$aVi:w5yf:#a8p39	a52341abe87ef983f2d80c4157af42649e73f7a31949ea7285053b9c8bce27aa707daac0e3981f28
a"tUih'irAkAALi$aVi:w5yf:#a8p39	1dd6093fbce7603b79e7e231af2231c77127c98063c4d2ed1991d6690e40065c32587426d5e6a076

Знайшли прообраз для повідомлення за 20106 ітерацій:

>#zvD=8iU4KI6svxtPAr3G+a-+ZPUsj	b48bd7f99940d676bf1f161a921e8e84b27959379a9c5eeb21df68cd6495d35b57095644359c0e24

3.2 Атака “Днів народжень”

3.2.1 Перший варіант атаки

Сформоване повідомлення: NedashkivskaArinaVitalyivna5085
Зафіксоване геш значення:
96dd76fa0b3050f7c6c1c56d36f02d34a37e00f991fc705cffd0b41578a77ebb0a3b8d1d46afd277

Перші 30 повідомлень та їх геші:

Повідомлення	Геш-значення
NedashkivskaArinaVitalyivna50851	1cdfe25e143538c7fd4da857084d19979b09099415d6dc507aa3f8538bd3586b0b86882c2cec32cd
NedashkivskaArinaVitalyivna50852	0b00b9234dc7c585e6f5532765ab3f84a1fe1f9bd3a64936191c970a4de3d98b5bcd21a3c58ec085
NedashkivskaArinaVitalyivna50853	c0caea3811b26ec13f41d4cb605c233811dff74a2fd5e628201362b71317e0e783a04b67b49fee03
NedashkivskaArinaVitalyivna50854	81c21a8c36c3f0ea4f1ac103d63da0126a4a7d5058ce6f2ea8d3acbf9d5ef26e02609d31e19f223d
NedashkivskaArinaVitalyivna50855	588c29a781ed4ed2693df244a4d76023dd39f775c005cb76b294936d35b619f94afee569f4838754
NedashkivskaArinaVitalyivna50856	138953f796a8617dbdef6c1e375b0b88ce709dca2cefcb033e732aaf95efe1c56c5007cacd0dcf43
NedashkivskaArinaVitalyivna50857	097f4e4315d8211741983c54c8d9ff815f61ac6fdf55761647bb66d2908b489951132e8a3739f29f
NedashkivskaArinaVitalyivna50858	88420c7359cc3644f37f35c80d335c033f6bcb7cf478c8ddbabaa58f906a76aa1fecae4df40eceb5
NedashkivskaArinaVitalyivna50859	9c686017d19eda16dedf7ff5449ad648fc4a4abbdda10f28483cb68513f8893a76ca841ca24e25bb
NedashkivskaArinaVitalyivna508510	8db27e2a6bbc9d681c12a59c48ea0fd7e7270357eb442a6db8022d0022304eeb6c74c92c84cb1cb5
NedashkivskaArinaVitalyivna508511	93835f5ae070eb4db13163bc4a0533691d319f302b71521f1a6a763627705f17552090cef7fad3c4
NedashkivskaArinaVitalyivna508512	99f44469efc78425740abd73c8b7aca4aae623dbc5df92a0e84a22a653ff3a03f6efd2a99c83e865
NedashkivskaArinaVitalyivna508513	332375a5f53cff0a6a79e3536c6217bcc3dbf1cdbbd08dba19c15742c4252d1b40aa3c102447ce58
NedashkivskaArinaVitalyivna508514	c1230ef940d7c665b59a56b1906e38ea2a725956d33480daae12e39fe994db4363f3ad01c2980b32
NedashkivskaArinaVitalyivna508515	5ab5eee88766b51ddabbd0c92a5fdc843697ee15629835089208e42634e20d7aafe4f8833859c544
NedashkivskaArinaVitalyivna508516	8106dfd902c731a1135bae12568ec8b71aa2c6471265b94b952a724ecdd765bf71777c589e8cdd1d
NedashkivskaArinaVitalyivna508517	dc7b8597609d581e36fd180dcc4b1352b7ad39b03e7031b383f0505824844a95710dc3b4e297fb7c
NedashkivskaArinaVitalyivna508518	a55f8b63fac851b694353b43a39d167d3e28ce314311d3b51f96504dc5a07e70a958fe70c898be49
NedashkivskaArinaVitalyivna508519	7297bc31fd16927d46c0e4ab5e43662169b367b531354bb7fd63b8af8946e62bfd258b449a8f7143
NedashkivskaArinaVitalyivna508520	fb7471ce4b72dd6cee41f672a132aefc07da682d3caedb6215ea8541bb43c8ce077cb0a4c0124353
NedashkivskaArinaVitalyivna508521	53c3f6de54be4fbdb4c7534319bc054e2a91a600dfd03e10e7472983457e3cd17f570b16f85db135
NedashkivskaArinaVitalyivna508522	95e5bb5446ae6e06615d323fb197a4d81765583af905860bc44e02a0e612c77930257b4db1c8f0ad
NedashkivskaArinaVitalyivna508523	91fde92627dcf5a0475b568d77a594eccabe385d620323e7841d2a3646c04c35c8d0dab2d10a50f6
NedashkivskaArinaVitalyivna508524	76d6ce5e1ab5d5a4be1575449707f75bcd54e1a82fbbff397a82a12198632b2c29563130808af81a
NedashkivskaArinaVitalyivna508525	78941eee72dcfff6f7736e9e8fc6bd426940976354198904bf0b66bb777c1452cfd1ee5d0155e36d
NedashkivskaArinaVitalyivna508526	c7d13f2eed0d6084d624ed86031f3202686ebddd1be29054ef4bda236facfd68bf939353515159 54
NedashkivskaArinaVitalyivna508527	e90434a22cd5ccc1117426f64152edaeee8d8672bdb07d1863c33c53f92c596523df8b5f0164e780
NedashkivskaArinaVitalyivna508528	6e1bf3eee9e8178cb650d167d335d9ed6daf603f63f67298a279162caf793d99c27712f09eb8e4b9
NedashkivskaArinaVitalyivna508529	3c641b3a88d72f1dde83b3adffcf6391ed819c684e0d4a2d8c946d6903df51e8249c7fe32f76c462
NedashkivskaArinaVitalyivna508530	70396607602f055bf46f55a0821f2667e8372b3c7f4efc76d3e8dd7856e883f2ccfd98d8aae0d425

Знайшли колізію за 86458 ітерацій:

NedashkivskaArinaVitalyivna508586458	5397842d4cbcac6f6b1a6293aa3fd1733b2dc9e2fc83e58d09d04b17273d94d353492f69ee6b76ff
NedashkivskaArinaVitalyivna508526181	b74d87781dd61ba1b99d0c6759f2abb5a22745eb96a8c5340cb69003948f1bd89914cf55ee6b76ff

3.2.2 Другий варіант атаки

Сформоване повідомлення: NedashkivskaArinaVitalyivna1647
Зафіксоване геш значення:
93d562f30e8b63e3bcc3610e58817fbf2442f75f2037ae9241b2748143396b4a23077da533faef5f

Перші 30 повідомлень та їх геші:

Повідомлення	Геш-значення
NedashkivskaArinNVitalyivna1647	99d31f32d8d8737a0bf333c33eb70e89adc79571586fff09eee03d6f653362135a8ceba8b3cb6284
NedashkivskaArinNVita3yivna1647	1bec1c4f297c8776ef912cf6f1013f79fc12375466dbec7693af73aa95086bc869c1c51ba91a3f5f
NedashkivskaArinNVita3yivnE1647	c48beed7a7db70977f01608c0ddae2afa2f9b6e943ce7faa57e6bb624da36a1bc87b76b3cccc7c35
NedashkivikaArinNVita3yivnE1647	a498b0c60188fcad22708061f41457f9391f8e43b00f570816c9e52ef334d76950664b3701e847ee
NedashkivikaApinNVita3yivnE1647	9bc70dc20975339949af162b022cd514502636f6eeabbcba1224f61eefd3ada92e5a5cea678eed83
NedashkivikaApinNVit/3yivnE1647	09815a654cc9a845486db45950b03294332d273bc3491c733faef89a9c46f485a0accd013c548e7f
NedashkivikaApinNVit/3yivnE164n	06ff1a5603792c771327f9586bcbc873672dc6d853dac7dad5ccdf43e9b29697790b0b6af412e007
NedashkivikaApiqNVit/3yivnE164n	47b077a70dae056025af83e3ca1008e21b595156a78e6eea94a74729ac6976e631c563dbd3a91d77
NedashkivikaApiqNVit/3yivnE16Nn	7ceb0132b246cc99b587bbe095536ce1d373caef0447024c7941b2d7dff28513cde07f871f4e78c7
NedashkijikaApiqNVit/3yivnE16Nn	2656ff546bcf1bd8ee8ee854497926e147d21726afd75ce2fa3d0fef06b82634703efbebb5075366
NedashkijikaApiqNVit/*yivnE16Nn	4fca82637a1f81cabbc3cab02048774d13036a46765e462d10634d2a33dcfdfb03badf989c80c40c
NedashkijikaApiqNViA/*yivnE16Nn	1f313e42a9ba5e62e02dcf4889b1871746719c597672c52425208aa1f3f7b2fa18c0e28687cc2cb1
NedashkijikaApiqNViA/*yivbE16Nn	008958ad91cb4cdda5cf3b33ffe41e8cb9c13762aa812c4b90bac1a96ae9214a6409910d54fa2911
NedashkijikaApiqNVis/*yivbE16Nn	dd946d6c255c2278886185b7981dfe4a0bbdc717388001188b451ffdc6bbfe6a7cf8ddcd1380a3b4
NedashkijikaApiqNVis/4yivbE16Nn	0115fce0ddfd4b48e503379bc6120bb904ec3a6aa2cfaf43da097a62dc7310dc815ea7a3fad0bacc
Nedashkijik7ApiqNVis/4yivbE16Nn	755835b94f6215e2c9b81a43f59531d4c87d6ff74a2a87459c22ee1c7dae3d0db8f63a32d5b08955
Nedas!kijik7ApiqNVis/4yivbE16Nn	799afc3b02f1192a5f2ffaa06523d07769940540595ba4c34741a2c4c3a4ad8881601227e8e0693b
Nedls!kijik7ApiqNVis/4yivbE16Nn	0cc5059dbf93e77d2ca1e99e5a7fd1da4e88c0f2509df2218551c9fc70f57bd1db4deddf3633ab74
Nedls!kijik7ApiqNVis/yyivbE16Nn	8a92a90aca2f9ae136d862415e73f27a2d4c3752639197abbed5cf67788418c612088e4b2fc621cc
Nedls!kijik7ApiqNVis/yyivbE16NY	f0ee9efcd84caa37b103a9e32e007550cc448648d5d98f9f14f2bfd0859546b85279ebb7836db488
Nedls!kijik7ApiqNVis/yyivbEq6NY	599c7884a24b3f8c8bea71286a3f4313e5d4c36d6609b12faf73d8107cb5f2e543981b404ec15458
Nedls!kijxk7ApiqNVis/yyivbEq6NY	3ce0327e34d48d9b51f9d6270e23d90014f4b24689441c880134ac64840e84c4049eef899f4351ff
Nedls!kijxktApiqNVis/yyivbEq6NY	0e01bee0e93b502089d9e0d37f86577691e4baa7fdac1a1a25d0438b941cdfe72ebe3d727f7611b9
Nedls7kijxktApiqNVis/yyivbEq6NY	92438849093c52eb02060e7d7f219fcf927ad3f67f0195369f6d174f36d900466429059c9a5aa2f7
Nedls7kijxktApiqNVis/yyivIEq6NY	d0378ac7238518dcb9b0bec1bf303d0d869e7dd3815a819c32b13d05ea9dc8b8ac8ad8c0771daf03
Nedls7kqjxktApiqNVis/yyivIEq6NY	922bd0550696589b7f6d2e8abf9b0c79916839bad363663da5edb3e9c54c2a9f84dabc9a763a5431
Nedls7kqjxkt2piqNVis/yyivIEq6NY	3a0c77f9db9ee3e844c685c1af1a86d690ab06b3870e423e37de40e1371aa2f9126efef37628e661
Nedls7kqjxkt2piqNVis/yyi4IEq6NY	fc24e86f1e406d511a0622f55d507663d5970426d445c1700cf45630b6fac62bf1d36fc62277b9c9
Nedl+7kqjxkt2piqNVis/yyi4IEq6NY	ddcc3ae0dedab9637ab2889ae6307a9f957864745ba3f5a7f6fca7faca24bb3805db367093518c53
4edl+7kqjxkt2piqNVis/yyi4IEq6NY	26e2320d2d85520f91eedb7fee1ce9b2001bd45c4fc8e5ec09d85f3388692ed4fcd7720dc43ae472

Знайшли колізію за 88674 ітерацій:

aN}v%}ES=<no9&[G!x_-Wz?;d,vE>]U	394fc5ea9c72bc2572b0b74ab0d41f8cf9e18ce233c374bcfc39550b76a8e00489abc14b777f51cd
IDnDoL9%56*"|W8h_O&qHkSh5]^rlf.	8afd868417bdc04e5f7b0a42cb5b80626cffad6bfd9600f40ac94f59dec850026fe7ed70777f51cd

4 Аналіз результатів при 100 запусках

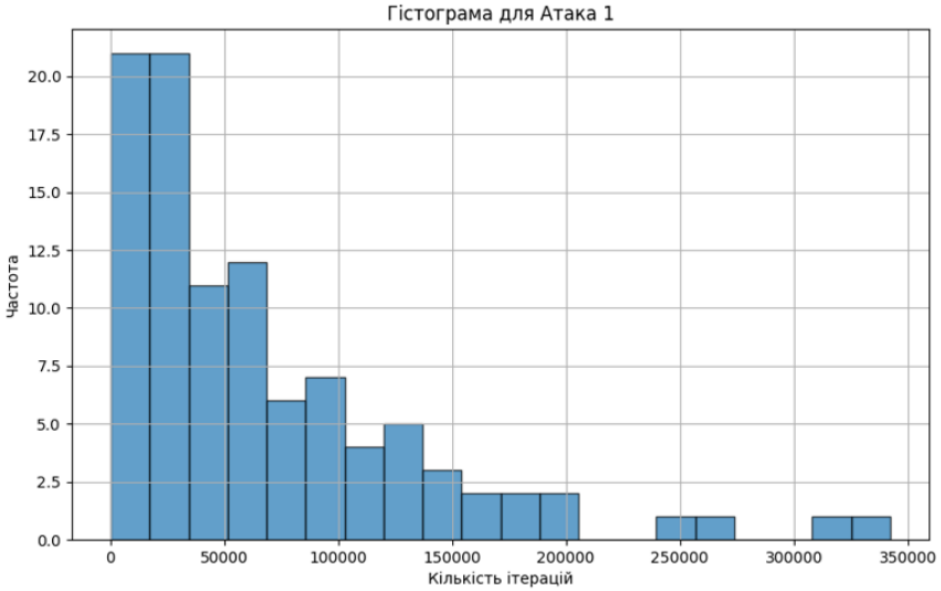
4.1 Випадковий пошук прообразу

4.1.1 Перший варіант атаки

Спочатку виведу кількість ітерацій атаки:

1	14753	21	34392	41	18443	61	108025	81	77089
2	29530	22	9820	42	125616	62	61631	82	138806
3	254046	23	35329	43	191505	63	3166	83	62166
4	147863	24	43243	44	26690	64	100504	84	161986
5	262773	25	34421	45	31538	65	94282	85	83393
6	342229	26	58969	46	40926	66	17412	86	55882
7	6430	27	7385	47	112962	67	125088	87	312827
8	8692	28	3414	48	195635	68	30656	88	9982
9	65136	29	14838	49	9931	69	79508	89	17986
10	28039	30	21669	50	23529	70	148238	90	112289
11	2131	31	36077	51	47148	71	36024	91	30025
12	19891	32	62657	52	76245	72	29618	92	2247
13	6235	33	90220	53	37722	73	61613	93	14042
14	120917	34	67116	54	2926	74	117208	94	172331
15	97632	35	16432	55	347	75	129006	95	21940
16	69128	36	33876	56	61636	76	581	96	22730
17	99646	37	5558	57	24599	77	17479	97	53065
18	173668	38	51023	58	29133	78	136255	98	101241
19	40207	39	37166	59	157263	79	24001	99	7424
20	57442	40	36188	60	55247	80	73582	100	102838

Тепер гістограма:



Для цієї атаки розподіл має сильний пік біля 0-50000 ітерацій. Це вказує на те, що більшість атак завершуються за порівняно невелику кількість ітерацій.. Також є окремі випадки, коли кількість ітерацій сягає 240000-270000 і 300000-350000.

Статистика	Значення
Середнє значення	67693.88
Дисперсія	4523817989.8056
0.95-Довірчий інтервал	(54348.16896297157, 81039.59103702844)

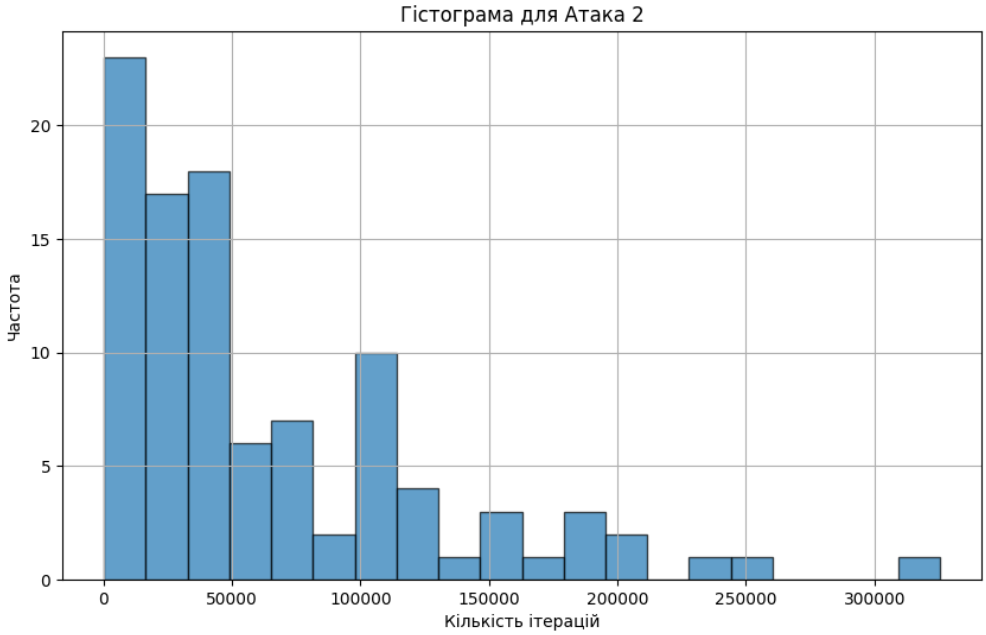
Теоретична оцінка у $O(2^n)$ для n=16 біт становить 65536 ітерацій. Отримане середнє значення доволі близьке до теоретичної оцінки, що підтвержує коректність теоретичної “моделі”. Невелике відхилення від теоретичного значення (приблизно 3.29%) може бути викликане випадковістю або розподілом випадкових значень.

4.1.2 Другий варіант атаки

Спочатку виведу кількість ітерацій атаки:

1	9776	21	42221	41	69527	61	10666	81	112184
2	39719	22	15865	42	162536	62	244	82	8357
3	23504	23	51318	43	112039	63	49150	83	111996
4	102163	24	38934	44	1689	64	21482	84	43670
5	28966	25	25161	45	71583	65	94600	85	128759
6	183355	26	148918	46	73248	66	45520	86	16286
7	3695	27	34918	47	70534	67	205696	87	11447
8	52431	28	31200	48	248321	68	9427	88	46956
9	29529	29	9528	49	57422	69	9006	89	101776
10	28200	30	74022	50	8282	70	91754	90	37986
11	196850	31	34637	51	111378	71	70516	91	17536
12	45622	32	4483	52	228458	72	30447	92	40678
13	64847	33	193857	53	23139	73	46120	93	71476
14	123033	34	153936	54	10350	74	182580	94	34035
15	120109	35	116920	55	102364	75	17894	95	6733
16	6286	36	42041	56	59573	76	3344	96	35239
17	3370	37	3905	57	141438	77	38408	97	27375
18	42671	38	41292	58	173727	78	325410	98	111039
19	31595	39	17042	59	105131	79	12472	99	7953
20	98758	40	30198	60	23368	80	11880	100	23579

Тепер гістограма:



Для цієї атаки розподіл має сильний пік біля 0-50000 ітерацій. Це вказує на те, що більшість атак завершуються швидко. Також є окремі випадки, коли кількість ітерацій сягає 250000 і 320000.

Статистика	Значення
Середнє значення	64706.58
Дисперсія	3986162889.3035994
0.95-Довірчий інтервал	(52179.01466586574, 77234.14533413426)

Теоретична оцінка у $O(2^n)$ для n=16 біт становить 65536 ітерацій. Отримане середнє значення доволі близьке до теоретичної оцінки, що підтвержує коректність теоретичної “моделі”. Невелике відхилення від теоретичного значення (приблизно -1.26%) може бути викликане випадковістю або розподілом випадкових значень.

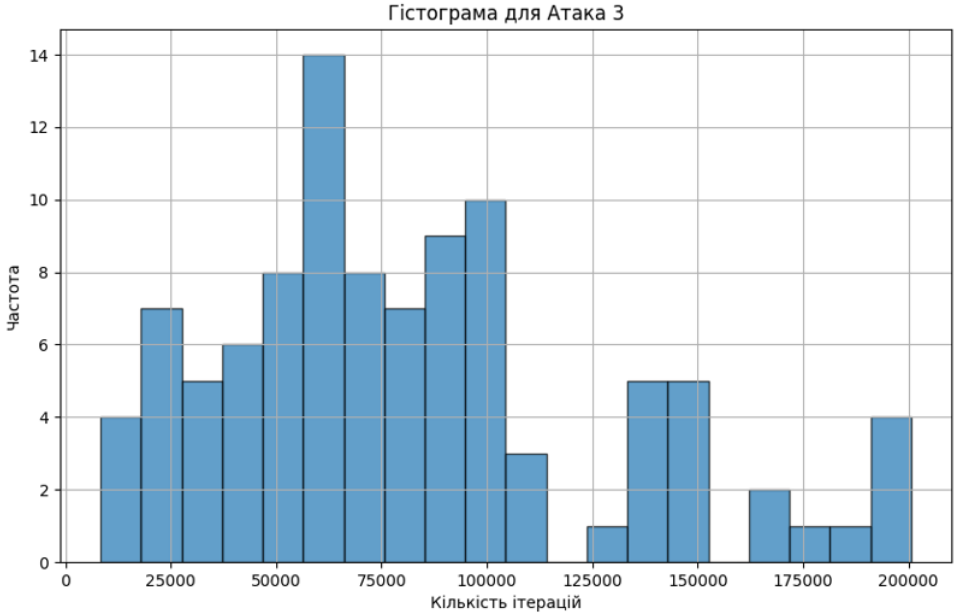
4.2 Атака “Днів народжень”

4.2.1 Перший варіант атаки

Спочатку виведу кількість ітерацій атаки:

1	103422	21	49482	41	22100	61	17790	81	103868
2	64335	22	23552	42	149648	62	101672	82	76453
3	136311	23	84918	43	61606	63	87240	83	67898
4	41505	24	46585	44	101907	64	59541	84	145549
5	102840	25	138722	45	45189	65	97361	85	74457
6	60713	26	70522	46	90397	66	81160	86	140615
7	59493	27	166897	47	151540	67	31135	87	61797
8	86060	28	89711	48	200594	68	74962	88	27593
9	97930	29	43210	49	66052	69	105173	89	50827
10	88469	30	170054	50	86189	70	25895	90	71826
11	61214	31	86526	51	188009	71	59328	91	132537
12	8350	32	102762	52	149203	72	198564	92	57907
13	80668	33	191658	53	92698	73	25886	93	46149
14	62551	34	22669	54	32911	74	35073	94	94929
15	71278	35	137975	55	140012	75	197292	95	54835
16	94489	36	49723	56	16366	76	23781	96	65371
17	146592	37	49928	57	66979	77	59240	97	56100
18	84027	38	15762	58	61246	78	33973	98	105320
19	180172	39	77641	59	101124	79	44911	99	77226
20	114019	40	27487	60	62585	80	51327	100	52140

Тепер гістограма:



Для цієї атаки розподіл більш рівномірний, із декількома піками, зокрема в діапазоні 50000-100000 ітерацій. Це вказує на більшу варіативність в кількості ітерацій.

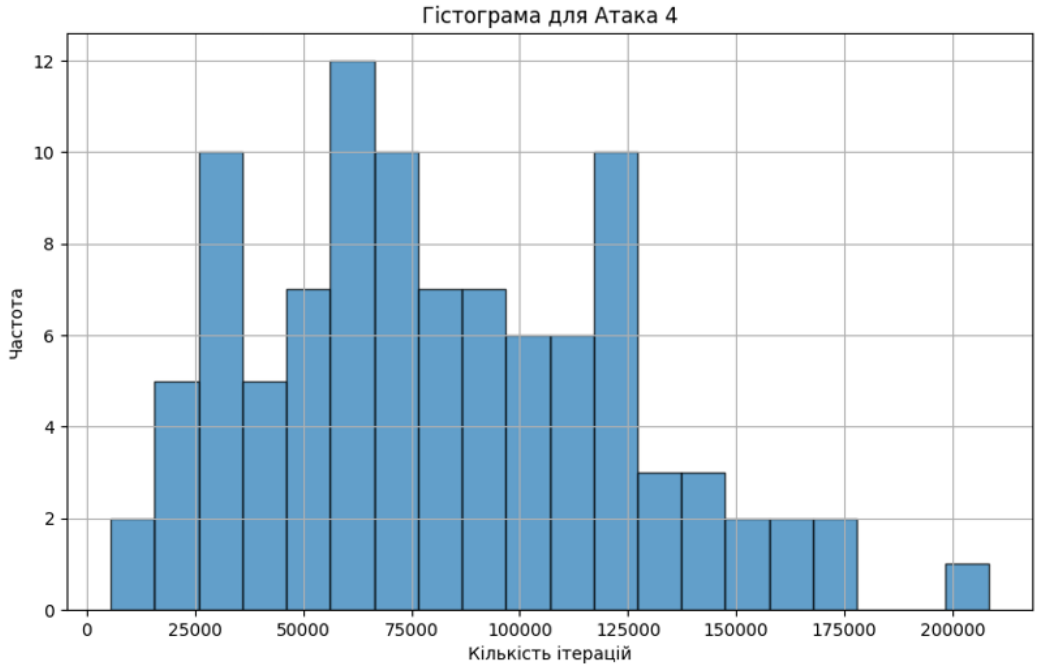
Статистика	**Значення**
Середнє значення	82512.78
Дисперсія	2127883375.8116
0.95-Довірчий інтервал	(73359.7883454598, 91665.77165454019)

4.2.2 Другий варіант атаки

Спочатку виведу кількість ітерацій атаки:

1	52252	21	102274	41	40005	61	124718	81	154252
2	91727	22	172787	42	118177	62	79012	82	106226
3	23901	23	82292	43	97248	63	73865	83	124560
4	68646	24	29697	44	112442	64	77142	84	19068
5	124672	25	72846	45	27386	65	34814	85	66595
6	69713	26	116537	46	19859	66	18063	86	169237
7	81524	27	60408	47	107430	67	146482	87	136848
8	39062	28	58036	48	95075	68	51823	88	39569
9	143170	29	45051	49	73129	69	51908	89	111534
10	82206	30	51338	50	34266	70	123590	90	122089
11	96113	31	46262	51	42053	71	62780	91	56748
12	65829	32	5541	52	87191	72	76233	92	76415
13	48947	33	72632	53	79834	73	80088	93	30883
14	62460	34	117446	54	29157	74	121340	94	34967
15	112490	35	14332	55	97686	75	57717	95	55822
16	91550	36	106858	56	30038	76	162490	96	17104
17	61002	37	93875	57	30536	77	154148	97	61247
18	144361	38	30812	58	63552	78	135181	98	107073
19	57798	39	119163	59	65086	79	123010	99	132463
20	90351	40	161447	60	208330	80	103061	100	70443

Тепер гістограма:



Для цієї атаки розподіл ще більш рівномірний, із декількома піками, зокрема в діапазоні 25000-125000 ітерацій. Це вказує на більшу варіативність в кількості ітерацій.

Статистика	**Значення**
Середнє значення	81764.96
Дисперсія	1769750207.3784003
0.95-Довірчий інтервал	(73417.67692758438, 90112.24307241563)

Атаки “днів народжень” мають трохи більше ітерацій, ніж атаки пошуку прообразу. Це може бути спричиненим тим, що розмір геш-значення (“суфікса”) розглядався в два рази більший. Також через те, що атаки “днів народжень” не заходили дальше 200000 і 210000 ітерацій вони мають в два рази меншу дисперсію.

5 Висновок

Під час виконання лабораторної роботи, я зрозуміла як використовувати геш-функції. Для атаки пошуку прообразу результати які у мене вийшли узгоджуються з теоретичним значенням, тоді як для атаки днів народжень спосперігається незначне відхилення. Проведений аналіз дозволяє зробити висновок про коректність реалізації атак і можливість використання теоретичних оцінок для оцінювання ефективності геш-функцій.