МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**Заняття № 3/19**. Перевірка криптостійкості AES

**РОБОТА З WEB-ДОДАТКОМ CYBERCHEF.IO**

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Петренко К.В.

18.05.2024

**Перевiрив:** викладач кафедри № 33

капітан \_\_\_\_\_\_\_\_\_\_\_\_Прийма О.О.

Київ – 2024

1. Виконати криптоаналіз і виділити основні властивості режимів шифрування AES.

PlainText:

AES is a variant of the Rijndael block cipher[5] developed by two Belgian cryptographers. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

Changed text:

DES is a variant of the Rijndael block cipher[5] developed by two Belgian cryptographers. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bytes.

| Mode | Key | IV | Add data | Cyphertext | Cyphertext(first letter) | Cyphertext(last word) |
| --- | --- | --- | --- | --- | --- | --- |
| ECB | 1b1c826f575dc0cf9ef0bc1405cb48c0 |  |  |  |  |  |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 |  |  |  |  |  |
| CBC | 1b1c826f575dc0cf9ef0bc1405cb48c0 | 5505c4ea0c63c6058280dca7899c32cc |  |  |  |  |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 | 5505c4ea0c63c6058280dca7899c32cc |  |  |  |  |
| CFB | 1b1c826f575dc0cf9ef0bc1405cb48c0 | 5505c4ea0c63c6058280dca7899c32cc |  | c36e955bba1a0042b892d9cefa93720b30082823ef465f6e332dbc696c645bbb7ab0493d4292a8907cc8d76891a2b55d64459dc283a232279e2ed0d19aa479356bb06404df05c7c3c9b2a0a2f863c8d39a7fd57f5a3ca58feac4291307db3a5aba94e0b7c2fde8e23c3814b43dcc178357d6629427ced3496cd01d5cbbe01fd91989d23907dc3c4e523a8cbb2fd48ae7b15697da377352ea8dd6aa77957060cbd2534978caeb8fc530aecda13a63c0ac7a5c713d730b1080e5765d73d39fbeb191bb428eabb70e535d2998c6dcb491e816aad1e9d25761a8f3e857fdeebb330259a8d7836a9a64ef882a7d1ccafe163bf321 | c66e955bba1a0042b892d9cefa93720ba97db0d6470ef13401139feeec8bb2b591a822e2a233a18379aecef0bab715daa85ccac4ba8baa08e35212754720ab54ce3e3fc061e431e9758d485e9c13c05a3c2c3451fc4285a740d7a5f41c5f1020070f6e91c8b194896fcbd2114b4dbb9c56b06860aa6e8f08cc38381ffe6f8f2083a729055b8bb458b8035b9cb3c9e95972e938b867c5571c2ff6044fbe2368e9bc71fc0944e209e67d07190756737f9ab7a89178f5bb4a233af147cfa82cb12996476feb2a9eed66b25c7220c9840e0755c1c6118cdae7c3d4ef86cab81eaf508a488b7469bfb7ced692156e530db72df85a | c36e955bba1a0042b892d9cefa93720b30082823ef465f6e332dbc696c645bbb7ab0493d4292a8907cc8d76891a2b55d64459dc283a232279e2ed0d19aa479356bb06404df05c7c3c9b2a0a2f863c8d39a7fd57f5a3ca58feac4291307db3a5aba94e0b7c2fde8e23c3814b43dcc178357d6629427ced3496cd01d5cbbe01fd91989d23907dc3c4e523a8cbb2fd48ae7b15697da377352ea8dd6aa77957060cbd2534978caeb8fc530aecda13a63c0ac7a5c713d730b1080e5765d73d39fbeb191bb428eabb70e535d2998c6dcb491e816aad1e9d25761a8f3e857fdeebb330259a8d7836a9a64ef882a7d1ccafe063bd6b573 |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 | 5505c4ea0c63c6058280dca7899c32cc |  | e58bb2171479df32abb269e51bd23f31d705187da70139e823cd004105e88bcb7257ab3e1595e6e23cbe23f3d3837b0c92944e95f8dd77f15ab3361cfbe01cd3458611ea7bcf2c1631018185839dc26544e7c5e63bd55080d6d18e177d978d3de08b47d80a578b456eead8ae3e5d9c24d310eb651d7a166fa1b654ce146262bb22955da0a2927ceeaf6a389dd7f9cfe964bfec4d55004f403e82ec151c9e249b583b7960d2698445dca10bf309220faa9d74af407b8b309fbb89031e577458a71ee2eb3812fe222418e0c5c090601b7278577f1981dd69bda080870ab66a9f859f5cc38b59cd535555e843e57ba06af330cd | e08bb2171479df32abb269e51bd23f3100d607608719c18c2573fb05ef0a5b5f31f40c46e0d0ccdb49dc4cc970ce2ad147433813047fd254130bf8bb406a08d782f223e57db62e73aa0c3fa0ce7c561a14f16bdd6fff1edea5ebf2376c209f76a274639c317135f8860dacf12fddacad7adb7dcdf5393d933dd293840fcaab32dad41d0417849128605725030755bc579063a2fd7e073ad4cac23f885da45c68c4abb08f817be519fe68f8fdcf982c3af578b19f9e782cfda2d031279782cee2c9c3739c7469e82bdc18fc9eb44d2e7b9d93e7c7b450c5a6ebe26b613a5a5a0ed0203d9c31a675519e78c818466818f66b9c | e58bb2171479df32abb269e51bd23f31d705187da70139e823cd004105e88bcb7257ab3e1595e6e23cbe23f3d3837b0c92944e95f8dd77f15ab3361cfbe01cd3458611ea7bcf2c1631018185839dc26544e7c5e63bd55080d6d18e177d978d3de08b47d80a578b456eead8ae3e5d9c24d310eb651d7a166fa1b654ce146262bb22955da0a2927ceeaf6a389dd7f9cfe964bfec4d55004f403e82ec151c9e249b583b7960d2698445dca10bf309220faa9d74af407b8b309fbb89031e577458a71ee2eb3812fe222418e0c5c090601b7278577f1981dd69bda080870ab66a9f859f5cc38b59cd535555e843e57ba07af330b954 |
| OFB | 1b1c826f575dc0cf9ef0bc1405cb48c0 | 5505c4ea0c63c6058280dca7899c32cc |  | c36e955bba1a0042b892d9cefa93720b9a2b6203cd0b4684e88dd2d5077915cdc4abdb73c6b3526f1996734c30a53e948f65f4b05301ae55b3db2e4f0402277342a1b460a5036b819bb352477a8f42553f16dfd47d82a40636bf2484fa0f1f57f531fcd79f4549400dfaec12cb17a53ca4d340401f3b034859357d1d069b4c8dbd65da223a889df88c14610b8e292600a157508922f73ee6ab0e4b19617495625c2798fcf31b8f26235caa99a3d7eb5179af5da99250ad16307ad25935d977d7e6168465f7650b12af9616b4f6c1ec35418f2eeed9f29d214a04657cbdf887be54b4a9cce2b5dfb55e6e1279e71fcfcc7cd5 | c66e955bba1a0042b892d9cefa93720b9a2b6203cd0b4684e88dd2d5077915cdc4abdb73c6b3526f1996734c30a53e948f65f4b05301ae55b3db2e4f0402277342a1b460a5036b819bb352477a8f42553f16dfd47d82a40636bf2484fa0f1f57f531fcd79f4549400dfaec12cb17a53ca4d340401f3b034859357d1d069b4c8dbd65da223a889df88c14610b8e292600a157508922f73ee6ab0e4b19617495625c2798fcf31b8f26235caa99a3d7eb5179af5da99250ad16307ad25935d977d7e6168465f7650b12af9616b4f6c1ec35418f2eeed9f29d214a04657cbdf887be54b4a9cce2b5dfb55e6e1279e71fcfcc7cd5 | c36e955bba1a0042b892d9cefa93720b9a2b6203cd0b4684e88dd2d5077915cdc4abdb73c6b3526f1996734c30a53e948f65f4b05301ae55b3db2e4f0402277342a1b460a5036b819bb352477a8f42553f16dfd47d82a40636bf2484fa0f1f57f531fcd79f4549400dfaec12cb17a53ca4d340401f3b034859357d1d069b4c8dbd65da223a889df88c14610b8e292600a157508922f73ee6ab0e4b19617495625c2798fcf31b8f26235caa99a3d7eb5179af5da99250ad16307ad25935d977d7e6168465f7650b12af9616b4f6c1ec35418f2eeed9f29d214a04657cbdf887be54b4a9cce2b5dfb55e6e1279e71fdfcc6a8854 |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 | 5505c4ea0c63c6058280dca7899c32cc |  | e58bb2171479df32abb269e51bd23f31b793e2d4a09c2d1e88fbabe1d29f23ed7351fd2470f93a731274ca6dc8b6c41dbd60f40ee79b2ebd1eb232c9a598f383cbc18bc3a62088f5bddedd65a7eb4815bde0ed989d7d744443fdf6f15f53502d4e616e44f877726c61d37ea777e6a1172c15592c0afc2d8f01d285892809e29ef482926d8ec63bfffcd459fed9611dd91e336903b26e5c7b91335e6f512a379fbbe522831607a3fd6a686024771aaa4e4581779a7d2eac6b26db1058038878837fcae342b461eed693e6abb7ebc3d57c189c5458fe5a5b9e56fa9e07124164e319b431d4ff3646e5036f744df6cd00ebd305 | e08bb2171479df32abb269e51bd23f31b793e2d4a09c2d1e88fbabe1d29f23ed7351fd2470f93a731274ca6dc8b6c41dbd60f40ee79b2ebd1eb232c9a598f383cbc18bc3a62088f5bddedd65a7eb4815bde0ed989d7d744443fdf6f15f53502d4e616e44f877726c61d37ea777e6a1172c15592c0afc2d8f01d285892809e29ef482926d8ec63bfffcd459fed9611dd91e336903b26e5c7b91335e6f512a379fbbe522831607a3fd6a686024771aaa4e4581779a7d2eac6b26db1058038878837fcae342b461eed693e6abb7ebc3d57c189c5458fe5a5b9e56fa9e07124164e319b431d4ff3646e5036f744df6cd00ebd305 | e58bb2171479df32abb269e51bd23f31b793e2d4a09c2d1e88fbabe1d29f23ed7351fd2470f93a731274ca6dc8b6c41dbd60f40ee79b2ebd1eb232c9a598f383cbc18bc3a62088f5bddedd65a7eb4815bde0ed989d7d744443fdf6f15f53502d4e616e44f877726c61d37ea777e6a1172c15592c0afc2d8f01d285892809e29ef482926d8ec63bfffcd459fed9611dd91e336903b26e5c7b91335e6f512a379fbbe522831607a3fd6a686024771aaa4e4581779a7d2eac6b26db1058038878837fcae342b461eed693e6abb7ebc3d57c189c5458fe5a5b9e56fa9e07124164e319b431d4ff3646e5036f744df6cd10ebc55865 |
| CTR | 1b1c826f575dc0cf9ef0bc1405cb48c0 | 5505c4ea0c63c6058280dca7899c32cc |  | c36e955bba1a0042b892d9cefa93720bffe3698cba2cec154a41a9be07bf5a506ac2b53d5c7d6b369df441de380774c7e861ba0e185a30bb41f760b29dfc63c3f09aa2398085979b65ed8e132d365d78c59e4686b3a189cb5fbe8d66297a881957160c2558f68e872cc1ced21bfb1e7695565b52621b95dc6f46650539a7b7a869940072b5a2adc72287a6d4a83925131e1138bb1bc97109adc05d46f27dacee86d25cdb01ce64a76ad98963ed8335c9ef3448a052da69dbca5861b8bfc6fbfdf98a55c2411d21738f6c27c292f416f145801861079db50eb2eb5b1a7400b3b74655799ee70a4f8219f444370351a553d3d6 | c66e955bba1a0042b892d9cefa93720bffe3698cba2cec154a41a9be07bf5a506ac2b53d5c7d6b369df441de380774c7e861ba0e185a30bb41f760b29dfc63c3f09aa2398085979b65ed8e132d365d78c59e4686b3a189cb5fbe8d66297a881957160c2558f68e872cc1ced21bfb1e7695565b52621b95dc6f46650539a7b7a869940072b5a2adc72287a6d4a83925131e1138bb1bc97109adc05d46f27dacee86d25cdb01ce64a76ad98963ed8335c9ef3448a052da69dbca5861b8bfc6fbfdf98a55c2411d21738f6c27c292f416f145801861079db50eb2eb5b1a7400b3b74655799ee70a4f8219f444370351a553d3d6 | c36e955bba1a0042b892d9cefa93720bffe3698cba2cec154a41a9be07bf5a506ac2b53d5c7d6b369df441de380774c7e861ba0e185a30bb41f760b29dfc63c3f09aa2398085979b65ed8e132d365d78c59e4686b3a189cb5fbe8d66297a881957160c2558f68e872cc1ced21bfb1e7695565b52621b95dc6f46650539a7b7a869940072b5a2adc72287a6d4a83925131e1138bb1bc97109adc05d46f27dacee86d25cdb01ce64a76ad98963ed8335c9ef3448a052da69dbca5861b8bfc6fbfdf98a55c2411d21738f6c27c292f416f145801861079db50eb2eb5b1a7400b3b74655799ee70a4f8219f444370351b553c58b16 |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 | 5505c4ea0c63c6058280dca7899c32cc |  | e58bb2171479df32abb269e51bd23f318ca58815af48a90532993e4f601636bd849e857d6a19087f0ac0f84d7a470304a7edc222aaf1aaa9d5782644c9dae6d96221d00b820438da2d40b7168c3860d9d36b8f910831e87c1dbb33e7e57b03855e0b91e59fc6dcfa5a69b82b09e2a0e17a4729eeb4ed327fdb2674862f32882afa68e05492cde4dedefba4e20c6fc739cda0181204a2ab097e0a0f2c655af1643a6702b2b04b7544cf0056de116ead808b1f59e909d44d924d81ab0c0f428cfbd00ec2f9fdb225dfe31227c98258a691673bbbd69e560b60115c2fcb4b8b6a220db0fd0de81d7d8de71ff749e8acc752163b | e08bb2171479df32abb269e51bd23f318ca58815af48a90532993e4f601636bd849e857d6a19087f0ac0f84d7a470304a7edc222aaf1aaa9d5782644c9dae6d96221d00b820438da2d40b7168c3860d9d36b8f910831e87c1dbb33e7e57b03855e0b91e59fc6dcfa5a69b82b09e2a0e17a4729eeb4ed327fdb2674862f32882afa68e05492cde4dedefba4e20c6fc739cda0181204a2ab097e0a0f2c655af1643a6702b2b04b7544cf0056de116ead808b1f59e909d44d924d81ab0c0f428cfbd00ec2f9fdb225dfe31227c98258a691673bbbd69e560b60115c2fcb4b8b6a220db0fd0de81d7d8de71ff749e8acc752163b | e58bb2171479df32abb269e51bd23f318ca58815af48a90532993e4f601636bd849e857d6a19087f0ac0f84d7a470304a7edc222aaf1aaa9d5782644c9dae6d96221d00b820438da2d40b7168c3860d9d36b8f910831e87c1dbb33e7e57b03855e0b91e59fc6dcfa5a69b82b09e2a0e17a4729eeb4ed327fdb2674862f32882afa68e05492cde4dedefba4e20c6fc739cda0181204a2ab097e0a0f2c655af1643a6702b2b04b7544cf0056de116ead808b1f59e909d44d924d81ab0c0f428cfbd00ec2f9fdb225dfe31227c98258a691673bbbd69e560b60115c2fcb4b8b6a220db0fd0de81d7d8de71ff749e8acd752006653 |
| GCM | 1b1c826f575dc0cf9ef0bc1405cb48c0 | 5505c4ea0c63c6058280dca7899c32cc | 6d204c3178d054724827bf1d7614e47f | 9ad6bc951887f368b1e6a61a2bb732cfa2fdfe9083eedea7cd9caea081840dc46c136c428093271679e880cd9f013f6b0fb271e97f4c3d36d993337eeee2c7d9c5eb3f4f2b3e0e3591385c7f45415d92a4fbacf79bed15161a3bdeb25b9cf817aa29792d1b29f81bdb986c905332cce9b65506c4937bb128353ba0c7b0581872503d8b233696fd1a91d900fecf48710cd09bb155703cc1cfc82a769d2317bb643f399d61c48a5b91f5605db6199101ab33a45f77b9c1c7f7c1072faa42768fb51cff2a89a6ff1f64cb2591a60ea1f6528e422caf91ad0dd8340a374a735f58e9053b2b6d89666138fcecaf2f7a59da060f2c  Tag: 4ab51d5ec8f64c72259d432cb332fad0 | 9fd6bc951887f368b1e6a61a2bb732cfa2fdfe9083eedea7cd9caea081840dc46c136c428093271679e880cd9f013f6b0fb271e97f4c3d36d993337eeee2c7d9c5eb3f4f2b3e0e3591385c7f45415d92a4fbacf79bed15161a3bdeb25b9cf817aa29792d1b29f81bdb986c905332cce9b65506c4937bb128353ba0c7b0581872503d8b233696fd1a91d900fecf48710cd09bb155703cc1cfc82a769d2317bb643f399d61c48a5b91f5605db6199101ab33a45f77b9c1c7f7c1072faa42768fb51cff2a89a6ff1f64cb2591a60ea1f6528e422caf91ad0dd8340a374a735f58e9053b2b6d89666138fcecaf2f7a59da060f2c  Tag: db6c770174a255d3f06845f93c05eb9e | 295adee8635df821eb8f7967a8e484768a0a15ed570036ffc62d688ee10b489c14abb1b4b142aa21fdb5bcec549762befd0fb68b4833b78952c7f9f30fecf146be1e8aa1f4e215eed6ecc79d979b30ecbb516beedd5b9cf1ecc0e75a5fee1de9ebbc74fb73e8679d6c9fa87f5c895cdbb11e7fcc218e43cffc343991949f51c7a928bff994035ead9c349157f7e9794d5532c32c0ae094e5bf5b3cacfb3b555ffa9641d0ab7e2115cdfccd8a559f72d2efe1f9b185c21c6943a0eae88b6b1ea9b5db235dd8f5f7ab3708b379b8062543bb48631630878266355fa0c367f0f3e18789181630b6ed45b275d0bc9a0088327be1  Tag: a41e85dd20569f0f6ffc81f3d3e75dbd |
| Change key | 1b1c826f575dc0cf9ef0bc1405cb48b2 | 5505c4ea0c63c6058280dca7899c32cc | 6d204c3178d054724827bf1d7614e47f | 2c5adee8635df821eb8f7967a8e484768a0a15ed570036ffc62d688ee10b489c14abb1b4b142aa21fdb5bcec549762befd0fb68b4833b78952c7f9f30fecf146be1e8aa1f4e215eed6ecc79d979b30ecbb516beedd5b9cf1ecc0e75a5fee1de9ebbc74fb73e8679d6c9fa87f5c895cdbb11e7fcc218e43cffc343991949f51c7a928bff994035ead9c349157f7e9794d5532c32c0ae094e5bf5b3cacfb3b555ffa9641d0ab7e2115cdfccd8a559f72d2efe1f9b185c21c6943a0eae88b6b1ea9b5db235dd8f5f7ab3708b379b8062543bb48631630878266355fa0c367f0f3e18789181630b6ed45b275d0bc9a0088327be1  Tag: abe6ed83a647afb121da7dcd8e626c66 | 295adee8635df821eb8f7967a8e484768a0a15ed570036ffc62d688ee10b489c14abb1b4b142aa21fdb5bcec549762befd0fb68b4833b78952c7f9f30fecf146be1e8aa1f4e215eed6ecc79d979b30ecbb516beedd5b9cf1ecc0e75a5fee1de9ebbc74fb73e8679d6c9fa87f5c895cdbb11e7fcc218e43cffc343991949f51c7a928bff994035ead9c349157f7e9794d5532c32c0ae094e5bf5b3cacfb3b555ffa9641d0ab7e2115cdfccd8a559f72d2efe1f9b185c21c6943a0eae88b6b1ea9b5db235dd8f5f7ab3708b379b8062543bb48631630878266355fa0c367f0f3e18789181630b6ed45b275d0bc9a0088327be1  Tag: a41e85dd20569f0f6ffc81f3d3e75dbd | 9ad6bc951887f368b1e6a61a2bb732cfa2fdfe9083eedea7cd9caea081840dc46c136c428093271679e880cd9f013f6b0fb271e97f4c3d36d993337eeee2c7d9c5eb3f4f2b3e0e3591385c7f45415d92a4fbacf79bed15161a3bdeb25b9cf817aa29792d1b29f81bdb986c905332cce9b65506c4937bb128353ba0c7b0581872503d8b233696fd1a91d900fecf48710cd09bb155703cc1cfc82a769d2317bb643f399d61c48a5b91f5605db6199101ab33a45f77b9c1c7f7c1072faa42768fb51cff2a89a6ff1f64cb2591a60ea1f6528e422caf91ad0dd8340a374a735f58e9053b2b6d89666138fcecaf2f7a59ca061971af  Tag: 81d45129549149bde911d4914d2b0e33 |

**Висновок:** У ході виконання завдання ми ознайомились і практично відпрацювали криптоаналіз шифрування алгоритму АES за допомогою сайту cyberchef.io. Шляхом криптоаналізу визначили основні відмінності у шифруванні у різних режимах АES та зміни шифротексту при зміні відкритого тексту, та ключа у кожному режимі шифрування.

Режим EBC: кожен блок даних шифрується незалежно один від одного. Це простий та швидкий режим, але не надійний для деяких типів даних, оскільки ідентичні блоки введення можуть виводити ідентичні дані.

Режим CBC: кожен блок даних комбінується з попереднім шифрованим блоком перед шифруванням. Це унеможливлює однаковість блоків виведення і додає безпеки, оскільки помилки в одному блоку не поширюються на всі наступні.

Режим CFB: дані шифруються блоками, але виведення шифру передається назад для генерації наступного блоку. Це дозволяє шифрувати невеликі порції даних і підтримує використання змінної довжини блоку.

Режим OFB: генерує блоки потоку ключів, які потім об'єднуються з блоками відкритого тексту, щоб отримати зашифрований текст. Перевертання біта в зашифрованому тексті призводить до перевернутого біта у відкритому тексті в тому ж місці. Ця властивість дозволяє багатьом кодам, що виправляють помилки, нормально функціонувати навіть при застосуванні до шифрування з помилками.

Режим CTR: генерує наступний блок потоку ключів, шифруючи послідовні значення "лічильника". CTR має схожі характеристики з OFB, але також дозволяє використовувати властивість довільного доступу під час дешифрування. Режим CTR добре підходить для роботи на багатопроцесорній машині, де блоки можуть бути зашифровані паралельно. Крім того, він не страждає від проблеми короткого циклу, яка може вплинути на OFB.

Просте додавання або XOR IV і counter в єдине значення в багатьох випадках порушить безпеку при атаці з обраним відкритим текстом, оскільки зловмисник може маніпулювати всією парою IV-лічильник, щоб викликати зіткнення. Як тільки зловмисник контролює пару IV-лічильник і відкритий текст, XOR зашифрованого тексту з відомим відкритим текстом дасть значення, яке, коли XOR з'єднається з шифротекстом іншого блоку, що має ту саму пару IV-лічильник, розшифрує цей блок. Однак, якщо інформація про зміщення/розташування пошкоджена, частково відновити такі дані буде неможливо через залежність від зміщення байтів.

Режим GCM: поєднує в собі добре відомий режим шифрування лічильника з новим режимом автентифікації Галуа. Ключовою особливістю є простота паралельного обчислення множення поля Галуа, що використовується для аутентифікації. Ця функція забезпечує вищу пропускну здатність, ніж інші алгоритми шифрування за рахунок використання паралельного шифрування. Блоки нумеруються послідовно, а потім цей номер блоку об'єднується з IV і шифрується блоковим шифром, важливо, щоб для кожного зашифрованого потоку використовувався окремий IV.

Блоки шифротексту вважаються коефіцієнтами многочлена, який потім обчислюється в ключовій точці H, використовуючи арифметику скінченного поля.

Потім результат шифрується, створюючи тег автентифікації, який можна використовувати для перевірки цілісності даних. Потім зашифрований текст містить тег IV, шифротексту та автентифікації.