```
1<sup>st</sup> column – lottery A
```

2nd column – lottery B

3rd column – tampered lottery A+B

```
07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa
                                                                                                                            d535fbc41300a4f2c7a72d70ba53aa2c
c0c86b2b375590849d8eb47d21e2e4aa
d535fbc41300a4f2c7a72d70ba53aa2c
0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fbe20b6cc85a8b663caf72e
                                                              989449f35ebf7adf40d32ddf77f27937
                                                                                                                            989449f35ebf7adf40d32ddf77f27937
                                                              9e6cdb79835ccaba4f59a3ff097c6d78
acf3d7c32e9ee945f66dda9df45b61c8
67c6360e9f13h74617936f0eed39e6c1
                                                                                                                            9e6cdb79835ccaba4f59a3ff097c6d78
7b82bc3d8064867db8ae917346470c1a
                                                                                                                            acf3d7c32e9ee945f66dda9df45b61c8
16d2f0c9409cff386de0ab9146986c5e
                                                              d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                            d6che2998d73ab7fe3342add58dc759c
f6d2b7dade603f007022388485ecc598
                                                              f6d2b7dade603f007022388485ecc598
                                                                                                                            f6d2b7dade603f007022388485ecc598
                                                                "info": {
                                                                                                                              "info": {
  "info": {
                                                             "lottery": "c369b7bf-c098-42ae-a8e6-
2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
238623550dbc",
                                                                                                                            "lottery": "9d69b7bf-c098-42ae-a8e6-
2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
238623550dbc",
"lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
"user": "21dc4ae1-f361-48d2-a2aa-
a70e0ab3c41b",
      "coin": 2
                                                                   "coin": 5
                                                                                                                                 "coin": 5
  }
                                                                                                                              }
                                                                }
```

```
d535fbc41300a4f2c7a72d70ba53aa2c
                                                             07cb5b1c4e405056c6cda62f47dea42c
                                                                                                                           d535fbc41300a4f2c7a72d70ba53aa2c
                                                              c0c86b2b375590849d8eb47d21e2e4aa
0eed4bcd220cede49b9004869f9c9751 c2f9f11a9fbe20b6cc85a8b663caf72e
                                                                                                                           0eed4bcd220cede49b9004869f9c9751
989449f35ebf7adf40d32ddf77f27937
                                                             989449f35ebf7adf40d32ddf77f27937
67c6360e9f13b74617936f0eed39e6c1
                                                             9e6cdb79835ccaba4f59a3ff097c6d78
acf3d7c32e9ee945f66dda9df45b61c8
                                                                                                                          9e6cdb79835ccaba4f59a3ff097c6d78
acf3d7c32e9ee945f66dda9df45b61c8
7b82bc3d8064867db8ae917346470c1a
16d2f0c9409cff386de0ab9146986c5e
                                                             d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                           d6cbe2998d73ab7fe3342add58dc759c
4db2948f1ad66ff7ff29ba80a87d8818
                                                             f2bd5e23e0bb870bb36936c0d0084753
                                                                                                                           f2bd5e23e0bb870bb36936c0d0084753
f6d2b7dade603f007022388485ecc598
                                                             f6d2b7dade603f007022388485ecc598
                                                                                                                           f6d2b7dade603f007022388485ecc598
                                                               "info": {
  "info": {
                                                                                                                             "info": {
"lottery": "<mark>9de5da56-9fad-4624</mark>-af1f-
5b91f4f2a2f7",
"user": "21dc4ae1-f361-48d2-a2aa-
                                                             "lottery": "c369b7bf-c098-42ae-a8e6-
2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
                                                                                                                          "lottery": "9de5da56-9fad-4624-a8e6-
2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
                                                             238623550dbc",
"coin": 5
                                                                                                                          238623550dbc",
"coin": 5
a70e0ab3c41b",
      coin": 2
  }
                                                                                                                             }
                                                               }
}
```

```
d535fbc41300a4f2c7a72d70ba53aa2c
                                                          07cb5b1c4e405056c6cda62f47dea42c
                                                                                                                    d535fbc41300a4f2c7a72d70ba53aa2c
                                                         c0c86b2b375590849d8eb47d21e2e4aa
989449f35ebf7adf40d32ddf77f27937
                                                                                                                   0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fbe20b6cc85a8b663caf72e
0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fbe20b6cc85a8b663caf72e
67c6360e9f13b74617936f0eed39e6c1
                                                         9e6cdb79835ccaba4f59a3ff097c6d78
acf3d7c32e9ee945f66dda9df45b61c8
                                                                                                                   9e6cdb79835ccaba4f59a3ff097c6d78
acf3d7c32e9ee945f66dda9df45b61c8
7b82bc3d8064867db8ae917346470c1a
16d2f0c9409cff386de0ab9146986c5e
4db2948f1ad66ff7ff29ba80a87d8818
                                                          d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                    d6cbe2998d73ab7fe3342add58dc759c
                                                          f2bd5e23e0bb870bb36936c0d0084753
                                                                                                                    f2bd5e23e0bb870bb36936c0d0084753
f6d2b7dade603f007022388485ecc598
                                                          f6d2b7dade603f007022388485ecc598
                                                                                                                    f6d2b7dade603f007022388485ecc598
                                                            "info": {
  "info": {
                                                                                                                      "info": {
    "lottery": "9de5da56-9fad-4624-af1f-
     "lottery": "<mark>9de5da56-9fad-4624-af1f-</mark>
                                                               "lottery": "c369b7bf-c098-42ae-a8e6-
5b91f4f2a2f7",
"user": "21dc4ae1-f361-48d2-a2aa-
                                                         2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
                                                                                                                   5b91f4f2a29d",
"user": "1ff3f8bd-44ba-4842-9d5f-
                                                         238623550dbc",
"coin": 5
                                                                                                                   238623550dbc",
"coin": 5
a70e0ab3c41b",
     "coin": 2
  }
}
```

```
d535fbc41300a4f2c7a72d70ba53aa2c
                                                        07cb5b1c4e405056c6cda62f47dea42c
                                                                                                                 d535fbc41300a4f2c7a72d70ba53aa2c
                                                        c0c86b2b375590849d8eb47d21e2e4aa
0eed4bcd220cede49b9004869f9c9751
                                                                                                                 0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fbe20b6cc85a8b663caf72e
67c6360e9f13b74617936f0eed39e6c1
                                                        989449f35ebf7adf40d32ddf77f27937
9e6cdb79835ccaba4f59a3ff097c6d78
                                                                                                                 c2f9f11a9fbe20b6cc85a8b663caf72e
                                                                                                                 67c6360e9f13b74617936f0eed39e6c1
7b82bc3d8064867db8ae917346470c1a
                                                        acf3d7c32e9ee945f66dda9df45h61c8
                                                                                                                 acf3d7c32e9ee945f66dda9df45b61c8
16d2f0c9409cff386de0ab9146986c5e
                                                        d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                 d6cbe2998d73ab7fe3342add58dc759c
4dh2948f1ad66ff7ff29ha80a87d8818
                                                        f2hd5e23e0hh870hh36936c0d0084753
                                                                                                                 f2bd5e23e0bb870bb36936c0d0084753
f6d2b7dade603f007022388485ecc598
                                                        f6d2b7dade603f007022388485ecc598
                                                                                                                 f6d2b7dade603f007022388485ecc598
                                                        {
   "info": {
        "'>++er
                                                        "lottery": "c369b7bf-c098-42ae-a8e6-
2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
                                                                                                                 "lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
"user": "21f3f8bd-44ba-4842-9d5f-
"lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
"user": "21dc4ae1-f361-48d2-a2aa-
a70e0ab3c41b",
                                                        238623550dbc",
                                                                                                                 238623550dbc",
     "coin": 2
                                                             "coin": 5
                                                                                                                      "coin": 5
  }
```

```
d535fbc41300a4f2c7a72d70ba53aa2c
                                                                07cb5b1c4e405056c6cda62f47dea42c
                                                                                                                               d535fbc41300a4f2c7a72d70ba53aa2c
 0eed4bcd220cede49b9004869f9c9751
                                                               c0c86b2b375590849d8eb47d21e2e4aa
989449f35ebf7adf40d32ddf77f27937
                                                                                                                              0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fbe20b6cc85a8b663caf72e
c2f9f11a9fbe20b6cc85a8b663caf72e
67c6360e9f13b74617936f0eed39e6c1
7b82bc3d8064867db8ae917346470c1a
                                                                                                                              67c6360e9f13b74617936f0eed39e6c1
7b82bc3d8064867db8ae917346470c1a
                                                                9e6cdb79835ccaba4f59a3ff097c6d78
                                                                acf3d7c32e9ee945f66dda9df45b61c8
16d2f0c9409cff386de0ab9146986c5e
4db2948f1ad66ff7ff29ba80a87d8818
                                                                d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                               d6cbe2998d73ab7fe3342add58dc759c
                                                                f2bd5e23e0bb870bb36936c0d0084753
                                                                                                                               f2bd5e23e0bb870bb36936c0d0084753
f6d2b7dade603f007022388485ecc598
                                                                f6d2b7dade603f007022388485ecc598
                                                                                                                               f6d2b7dade603f007022388485ecc598
{
    "info": {
                                                                  "info": {
                                                                                                                                 "info": {
                                                                                                                              "into": {
    "lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
    "user": "21dc4ae1-f361-48d2-9d5f-
238623550dbc",
"lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
"user": "2ldc4ae1-f361-48d2-a2aa-
                                                                     "lottery": "c369b7bf-c098-42ae-a8e6-
                                                               2ec6018cc79d",

"user": "1ff3f8bd-44ba-4842-9d5f-

238623550dbc",
a70e0ab3c41b",
"coin": 2
                                                                     "coin": 5
                                                                                                                                    "coin": 5
                                                                                                                                 }
  }
                                                                  }
```

```
d535fbc41300a4f2c7a72d70ba53aa2c
                                                        07ch5h1c4e405056c6cda62f47dea42c
                                                                                                                d535fhc41300a4f2c7a72d70ha53aa2c
                                                        c0c86b2b375590849d8eb47d21e2e4aa
0eed4bcd220cede49b9004869f9c9751
                                                                                                                0eed4bcd220cede49b9004869f9c9751
c2f9f11a9fhe20h6cc85a8h663caf72e
                                                        989449f35ehf7adf40d32ddf77f27937
                                                                                                                c2f9f11a9fhe20h6cc85a8h663caf72e
67c6360e9f13b74617936f0eed39e6c1
                                                        9e6cdb79835ccaba4f59a3ff097c6d78
                                                                                                                67c6360e9f13b74617936f0eed39e6c1
7h82hc3d8064867dh8ae917346470c1a
                                                        acf3d7c32e9ee945f66dda9df45b61c8
                                                                                                                7h82hc3d8064867dh8ae917346470c1a
16d2f0c9409cff386de0ab9146986c5e
4db2948f1ad66ff7ff29ba80a87d8818
                                                        d6cbe2998d73ab7fe3342add58dc759c
                                                                                                                16d2f0c9409cff386de0ab9146986c5e
f2bd5e23e0bb870bb36936c0d0084753
                                                        f2hd5e23e0hh870hh36936c0d0084753
f6d2b7dade603f007022388485ecc598
                                                        f6d2b7dade603f007022388485ecc598
                                                                                                                f6d2b7dade603f007022388485ecc598
                                                                                                                "into": {
    "lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
    "user": "21dc4ae1-f361-48d2-a2aa-
a70e0ab3c4bc",
"lottery": "9de5da56-9fad-4624-af1f-
5b91f4f2a2f7",
"user": "2ldc4ae1-f361-48d2-a2aa-
                                                             "lottery": "c369b7bf-c098-42ae-a8e6-
                                                        2ec6018cc79d",
"user": "1ff3f8bd-44ba-4842-9d5f-
238623550dbc",
a70e0ab3c41b",
    "coin": 2
                                                             "coin": 5
                                                                                                                     "coin": 5
  }
                                                          }
                                                                                                                  }
```

XX XX XX XX XX XX XX XX

Presumed structure of enc plaintext:

[70:7f] CC xx xx xx xx xx xx xx xx

```
{"lotteryid": "9d
e5da56-9fad-4624
-af1f-5b91f4f2a2
f7", "userid": "21
dc4ae1-f361-48d2
-a2aa-a70e0ab3c4
1b", "coingain":2
}###############
[00:0f] xx xx xx xx xx xx xx xx xx
                                   XX XX XX XX XX XX LL LL
                                   LL LL LL LL LL LL LL LL
[10:1f] LL LL LL LL LL LL LL LL
[20:2f] LL LL LL LL LL LL LL LL
                                   XX XX XX XX XX XX UU UU
[30:3f] LL LL xx xx xx xx xx xx xx
[40:4f] UU UU UU UU UU UU UU UU
                                  UU UU UU UU UU UU UU UU
[50:5f] UU UU UU UU UU UU UU UU
                                  UU UU UU UU UU UU UU UU
[60:6f] UU UU xx xx xx xx xx xx xx
                                   XX XX XX XX XX XX CC
```