

1st column – lottery A

2nd column – lottery B

3rd column – tampered lottery A+B

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9d69b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9de5da56-9fad-4624-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a29d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7f29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220cede49b9004869f9c9751c2f9f11a9fbe20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c1acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21f3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220ced49b9004869f9c9751c2f9f11a9fbc20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7ff29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220ced49b9004869f9c9751c2f9f11a9fbc20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7ff29ba80a87d8818f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-9d5f-238623550dbc", "coin": 5 } }

d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220ced49b9004869f9c9751c2f9f11a9fbc20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7ff29ba80a87d8818f6d2b7dade603f007022388485ecc598	07cb5b1c4e405056c6cda62f47dea42cc0c86b2b375590849d8eb47d21e2e4aa989449f35ebf7adf40d32ddf77f279379e6cdb79835ccaba4f59a3ff097c6d78acf3d7c32e9ee945f66dda9df45b61c8d6cbe2998d73ab7fe3342add58dc759cf2bd5e23e0bb870bb36936c0d0084753f6d2b7dade603f007022388485ecc598	d535fbc41300a4f2c7a72d70ba53aa2c0eed4bcd220ced49b9004869f9c9751c2f9f11a9fbc20b6cc85a8b663caf72e67c6360e9f13b74617936f0eed39e6c17b82bc3d8064867db8ae917346470c1a16d2f0c9409cff386de0ab9146986c5e4db2948f1ad66ff7ff29ba80a87d8818f6d2b7dade603f007022388485ecc598
{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b", "coin": 2 } }	{ "info": { "lottery": "c369b7bf-c098-42ae-a8e6-2ec6018cc79d", "user": "1ff3f8bd-44ba-4842-9d5f-238623550dbc", "coin": 5 } }	{ "info": { "lottery": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7", "user": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c4bc", "coin": 5 } }

Presumed structure of enc plaintext:

```
{
  "lotteryid": "9de5da56-9fad-4624-af1f-5b91f4f2a2f7",
  "userid": "21dc4ae1-f361-48d2-a2aa-a70e0ab3c41b",
  "coingain": 2
}#####
```

[00:0f]	xx xx xx xx xx xx xx xx	xx xx xx xx xx xx LL LL
[10:1f]	LL LL LL LL LL LL LL LL	LL LL LL LL LL LL LL LL
[20:2f]	LL LL LL LL LL LL LL LL	LL LL LL LL LL LL LL LL
[30:3f]	LL LL xx xx xx xx xx xx	xx xx xx xx xx xx UU UU
[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
[70:7f]	CC xx xx xx xx xx xx xx	xx xx xx xx xx xx xx xx