

Crossbones Cash

Kansas K.A.R. 111-23-14 · eInstant Cert Pack v1

Issued: 2026-05-15T21:45:32.661962Z · Authority: Multi.Bingo iLottery RGS
Signing key: Ed25519 · ID d651f1b9f793f40d

Math validation

Pool size	1,000,000
RTP @ unit denom	88.0000%
Top prize (max denom)	\$100,000
Bonus engine	generic_bonus

1. Game specification (Kansas K.A.R. 111-23-14)

Crossbones Cash is an instant lottery game governed by Kansas K.A.R. 111-23-14. Finite-pool model with 1,000,000 shares per pool. The bit-exact payable below has been imported from the K.A.R. (j) odds table.

Prize formula: $\text{prize_cents} = \text{multiplier} \times \text{denom_cents} \times \text{tickets_purchased}$

2. Paytable (59 tiers)

Multiplier	Count in pool	Odds (1 in)
×5000.0	2	500,000.00
×122.0	5	200,000.00
×121.0	12	83,333.33
×120.0	80	12,500.00
×118.0	4	250,000.00
×117.0	15	66,666.67
×115.0	5	200,000.00
×114.0	12	83,333.33
×113.0	100	10,000.00
×112.0	30	33,333.33
×110.0	3	333,333.33
×109.0	5	200,000.00
×108.0	50	20,000.00
×105.0	5	200,000.00
×70.0	50	20,000.00
×67.0	10	100,000.00
×62.0	15	66,666.67
×50.0	350	2,857.14
×45.0	50	20,000.00
×42.0	10	100,000.00
×40.0	15	66,666.67
×39.0	100	10,000.00
×38.0	750	1,333.33
×37.0	100	10,000.00
×36.0	35	28,571.43
... (34 more)		

3. Pool architecture

Each pool consists of 1,000,000 shares. Pool generation: RGS service `multibingo-rng:9443` provides the server seed (RNG_STRICT=true, no local fallback). Paytable counts written into array, shuffled with `mulberry32(SHA-256(server_seed))` Fisher-Yates. Pool audit_hash chained via Ed25519 signature. Tickets consumed sequentially; outcome = multiplier at position in shuffled array.

4. Audit chain (K.A.R. h)

Daily Merkle root signed with Ed25519 (key ID `d651f1b9f793f40d`). Leaves = ticket_hash + pool_hash. Persisted in WORM-locked PG row + audit blob to disk (S3 Object Lock in prod). Each day's row stores `prev_root_sha256` forming a hash chain.

5. Verifier endpoints

```
GET /api/ilottery/games/CROSSBONES_CASH/paytable
GET /api/ilottery/games/CROSSBONES_CASH/config?jur=GLI-SANDBOX
POST /api/ilottery/games/CROSSBONES_CASH/open-pool
POST /api/ilottery/games/CROSSBONES_CASH/play
POST /api/ilottery/vector/replay (game_code=CROSSBONES_CASH)
GET /api/ilottery/verify/:ticket_id
GET /api/ilottery/merkle/proof/:ticket_id
GET /api/ilottery/audit/public-key
```

6. Test vectors v1

URL: https://kobowlotto.com/mathforge/ilottery/gdd/crossbones_cash/vectors_v1.json
600 vectors × 5 denoms = 3,000 prize data points (6 tiers × 100 each).

7. Operator Ed25519 public key

```
-----BEGIN PUBLIC KEY-----
MCowBQYDK2VwAyEAU2k0zXnm09QHduKLSEQYUAFeACAEOTUceEuiRGLSiXs=
-----END PUBLIC KEY-----
```