Diamond Flare

Kansas K.A.R. 111-23-16 · eInstant Cert Pack v1

Issued: 2026-05-15T21:45:33.391590Z · Authority: Multi.Bingo iLottery RGS
Signing key: Ed25519 · ID `d651f1b9f793f40d`

Math validation

Pool size	1,000,000
RTP @ unit denom	88.0500%
Top prize (max denom)	$10,000
Bonus engine	wheel_spin

1. Game specification (Kansas K.A.R. 111-23-16)

Diamond Flare is an eInstant lottery game governed by Kansas K.A.R. 111-23-16. Finite-pool model with 1,000,000 shares per pool. The bit-exact paytable below has been imported from the K.A.R. (j) odds table.
Prize formula: prize_cents = multiplier × denom_cents × tickets_purchased

2. Paytable (25 tiers)

Multiplier	Count in pool	Odds (1 in)
×5000.0	1	1,000,000.00
×2500.0	1	1,000,000.00
×1000.0	1	1,000,000.00
×500.0	5	200,000.00
×250.0	10	100,000.00
×200.0	10	100,000.00
×100.0	50	20,000.00
×75.0	50	20,000.00
×60.0	150	6,666.67
×50.0	250	4,000.00
×45.0	50	20,000.00
×40.0	50	20,000.00
×35.0	500	2,000.00
×30.0	1,500	666.67
×25.0	500	2,000.00
×20.0	5,750	173.91
×15.0	8,000	125.00
×10.0	8,000	125.00
×8.0	5,000	200.00
×6.0	5,000	200.00
×5.0	12,000	83.33
×4.0	2,500	400.00
×3.0	2,500	400.00
×2.0	79,000	12.66
×1.0	135,000	7.41

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/DIAMOND_FLARE/paytable
GET /api/ilottery/games/DIAMOND_FLARE/config?jur=GLI-SANDBOX
POST /api/ilottery/games/DIAMOND_FLARE/open-pool
POST /api/ilottery/games/DIAMOND_FLARE/play
POST /api/ilottery/vector/replay (game_code=DIAMOND_FLARE)
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/diamond_flare/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-----
```