Money Heist Database Management System

1.1 Idea Formulation

Mini-World Setting and Database concept

Our database system is set in the universe of Money Heist, where a criminal mastermind known as "The Professor" orchestrates elaborate heists against government institutions. The mini world encompasses the Royal Mint of Spain during an active heist operation, including all internal and external locations, communication networks, and personnel involved. We propose the "Heist Command & Control Database System (HCCDS)" —a comprehensive system essential for coordinating the chaotic, high-stakes operation in real-time.

Core Entities

The database structure is built around ten critical entities necessary for operational control:

1. Hostages – STRONG ENTITY
2. Dependents**:** Must be linked to a Hostage - WEAK ENTITY
3. Team Members (Crew, Professor, Hacker) – STRONG ENTITY
4. Security System (Cameras, Alarms, Access Points) – STRONG ENTITY
5. Safe Houses (Preparation/Retreat locations) – STRONG ENTITY
6. Equipment (Weapons, Tools, Comms) – STRONG ENTITY
7. Mission **(Specific Tasks/Objectives)** – STRONG ENTITY
8. Police/Investigator (Law Enforcement Tracking) – STRONG ENTITY
9. Evidence (Compromise Tracking) - WEAK ENTITY
10. Loot (Production/Inventory) – STRONG ENTITY
11. Communication Log (Negotiations, Radio Traffic)

Novelty of the idea:

The HCCDS is special because it's built just for a big crime, copying The Professor's careful planning style with these key features:

- **Custom-Made Security:** Uses code names and team rules for secret access, instead of standard usernames.
- **Built-in Counter-Police:** Tracks police moves and evidence in real-time so the crew can always react quickly.
- **Flexible Planning:** The system can adjust the mission plan right away when things go wrong, instead of being stuck with old steps.
- **People Control:** Keeps notes on hostages and their families (psychological profiling) to use as a tool in talks.

1.2 User identification and Interaction

Primary Users:

1. The Professor (Database Administrator)

- Full access to all database modules
- Can create, modify, and delete any records
- Views real-time dashboards and analytics
- Manages user permissions and access levels

2. Team Leaders (Berlin, Tokyo, Nairobi)

- Access to team member information for their assigned groups
- Can update mission status and equipment requests
- View hostage information relevant to their zones
- Cannot access other leaders' operational data

3. Specialized Operators:

- Rio (Hacker): Access to security system logs and communication modules
- Moscow (Equipment Manager): Full access to equipment inventory and distribution logs
- Denver (Ground Operations): Access to hostage management and zone control data

4. External Negotiator (Raquel Murillo/Lisbon)

- Limited read-only access to communication logs
- Can input negotiation outcomes and agreements

Interaction Methods:

- Web-based interface accessible through encrypted VPN
- Mobile application for field operatives with offline sync capability
- Command-line interface for emergency access
- Automated alerts and notifications system

1.3 Purpose of the database

- **Why Essential:** Transforms chaotic operations into coordinated, data-driven missions.
- **Real-time Sync:** Guarantees all team members have the current information instantly, preventing fatal mistakes.
- **Complex Relations:** Efficiently tracks intricate relationships (e.g., Hostage ↔ Dependent leverage) that are too hard to track manually.
- **Instant Query:** Allows The Professor to get immediate, complex answers for fast tactical decisions.
- **Audit Trail:** Logs every action with a timestamp, crucial for security and avoiding police evidence.
- **Predictive Help:** Allows analysis of patterns (like police timing) to plan smarter.

2.Database requirements

1. The Building Blocks (Entities and Keys)

- **Total Entities:** 11
- **Entities with Two Keys:**

    - **Communication Log:** Needs both the time and the channel ID to uniquely mark a message.
    - **Loot:** Needs both the batch ID and the date it was made to track the money.
- **Weak Entities:** These entities can't exist on their own; they must be linked to another entity.
    - **Dependents:** Must be linked to a Hostage.
    - **Evidence:** Must be linked to a Police/Investigator who found it.

2. How Things Connect (Relationships)

The system uses strong connections (relationships) to link the data:

- **Has-Dependent (1:N):** One Hostage can have many Dependents.
- **Guards (M:N):** Many Team Members can guard many Hostages.
- **Assigned-To (M:N):** Many Team Members can be on many Missions.
- **Stored-In (1:N):** One Safe House can store many Loot batches.
- **Monitored-By (M:N):** Many Security Systems can monitor many Hostages.
- **Reports-To (1:N):** One Team Leader can have many Team Members reporting to them.
- **Collected-During (M:N):** Many Evidence items can be linked to many Missions.

3. The Mega-Relationships (N > 3)

We need complex links to track major events:

- **Mission Execution (4-way):** Tracks which **Team Member** used what **Equipment** during which **Mission** at what **Safe House**.
- **Resource Coordination (4-way):** Tracks which **Supplier** provided which **Resource** to which **Team Member** at which **Safe House**.
- **Strategic Planning (5-way):** Tracks which **Team Member** planned which **Mission** with which **Police/Investigator** through which **Communication Log**.

4. Data Rules (Constraints)

- **Primary Key Rule:** All main IDs (keys) must be **unique** (e.g., no two team members can have the same ID).
- **Linking Rule (Foreign Key):** If you link to a record (like a Hostage ID), that record must already exist.
- **Trivial common Rules:**
    - Age must be between 0 and 120.
    - Loot quantity cannot be a negative number.
    - Security Levels must be one of four options (Green, Yellow, Red, Compromised).
    - Mission stages must happen in the right order (e.g., must be Active before it can Fail).

3.Functional requirements

3.1 Retrieval Operations

3.1.1 Selection

- Retrieve all hostages with government positions captured today
- Display all team members currently inside the mint with their code names and roles
- Show all active missions in Zone 3
- List all evidence items with high threat level

3.1.2 Projection

- Show only the names and medical conditions of elderly hostages
- Display equipment type and quantity without location details
- List communication timestamps without revealing content
- Show mission codes without operational details

3.1.3 Aggregation

- SUM: SELECT SUM(l.amount) FROM Loot l JOIN Production_Schedule p ON l.batch_id = p.batch_id WHERE p.date = TODAY

- COUNT: SELECT COUNT(*) FROM Hostages h JOIN Behavioral_Assessment b ON h.id = b.hostage_id WHERE b.status = 'hostile'
- MAX: SELECT MAX(c.duration) FROM Communication_Log c JOIN Police p ON c.negotiator_id = p.id
- MIN: SELECT MIN(e.quantity) FROM Equipment e JOIN Equipment_Type et ON e.type_id = et.id WHERE et.critical = true
- AVG: SELECT AVG(response_time) FROM Police_Response pr JOIN Diversion_Events de ON pr.event_id = de.id

3.1.4 Search capabilities

The system requires robust Partial Text Matching to ensure rapid, real-time information retrieval during critical moments (e.g., typing "AK" for "AK-47" or "MAR" for hostages named Maria/Mario). This is essential for:

- Equipment Search
- Hostage Search
- Communication Log Search
- Evidence Search
- Mission Search

3.1.5 Additional query examples

- Find team members who have handled more equipment than the average across all members
- Group communication logs by type (negotiation, internal, emergency) and show frequency patterns with average duration
- List all hostages who have family members also held captive, along with their relationships and medical conditions

3.2 Analysis report

The system must generate a minimum of three comprehensive, intelligence reports utilizing JOIN Operations to correlate complex data:

Analysis Report	**Primary Goal**	**Key JOIN Operations**
1. Hostage Vulnerability Analysis	Identify high-risk individuals and map hostage-guard relationships for targeted strategies.	Hostages JOIN Dependents; Hostages JOIN Medical_Records; Hostages JOIN Zone_Assignments
2. Equipment Consumption Rate Analysis	Track burn rate of critical supplies and project depletion timelines for logistics planning.	Equipment JOIN Mission; Equipment JOIN Equipment_Requests; Equipment JOIN Delivery_Logs
3. Police Response Pattern Analysis	Predict likely assault windows by analyzing negotiation trends, police positioning, and investigation status.	Police JOIN Communication_Log; Police JOIN Evidence; Police JOIN Security_System

3.3 Modification Operations

The system requires comprehensive data manipulation capabilities to manage the dynamic nature of the heist:

Operation Type	**Examples (Critical for Heist Flow)**
Insertion (Adding Data)	Logging new **Hostages**, recording new **Team Members** (e.g., Lisbon), logging every **Communication Entry**, and creating new **Missions**.
Update (Changing Data)	Modifying **Hostage Status** (cooperative/resistant), adjusting **Safe House** security levels, updating **Mission Phase** progression, and changing **Loot Quantities**.
Deletion (Removing Data)	Removing released **Hostages**, clearing compromised **Safe Houses**, purging outdated **Communication Logs**, and eliminating false **Evidence** trails.

Key Differentiators:

The HCCDS is the superior solution because it is designed as a specialized command-and-control system, not a generic manager.

1. **Full Strategic Integration:** The database is not just themed; its entities and relationships must work together to create a cohesive, operationally realistic Heist

Management System, directly reflecting the complexity of the *Money Heist* narrative.

2. **Adaptive Security and Control:** The system enforces multi-tier, character-driven security (RBAC) and is dynamically structured to adapt to the fluid nature of the operation, ensuring the Professor always maintains control without single points of failure.
3. **Comprehensive Tactical Coverage:** It provides end-to-end management, from tracking loot production and equipment logistics to processing hostage psychological profiles and executing real-time counter intelligence against police movements.