1. To solve modular arithmetic problems, we use the fact that a x b mod m can be simplified by first reducing a and b modulo m and then multiplying and reducing the result modulo m
    a. 26 * 27 mod 13
        i. 26 modulo 13 = 0 (since 26 = 2×13)
        ii. 27 modulo 13 = 1 (since 27 = 2 × 13 + 1)
        iii. Multiply reduced values = 0 * 1 = 0
        iv. Thus 26 * 27 mod 13 = 0
    b. 16 * 24 mod 13
        i. 16 modulo 13 = 3
        ii. 24 modulo 13 = 11
        iii. Multiply reduced values = 3 * 11 = 33
        iv. Thus 16 * 24 mod 13 = 33
    c. 16^3 mod 13
        i. 16 modulo 13 = 3
        ii. 16^3 = 16 * 16 * 16
        iii. Multiplying reduced values = 3 * 3 * 3 = 27
        iv. Thus 16^3 mod 13 = 27
    d. -24*3 mod 13
        i. 24 modulo 13 = 11
        ii. 3 mod 13 = 3
        iii. Multiplying reduced values = 11 * 3 = 33
        iv. Thus -24*3 mod 13 = -33
2. Part 1
    a. Encryption equation
        i. The encryption part can be broken into the following steps:
            1. **Initial Setup**:
                a. An initialization vector (IV) is used as input to generate the first key stream output.
                b. The feedback structure ensures that each subsequent ciphertext depends on the previous ciphertext.
            2. **Feedback mechanism**
                a. The previous ciphertext, denoted as yi-1 is fed into the feedback loop to influence the current encryption of the next plaintext bit.
                b. The key k is combined with the feedback using some function, denoted ei, which could be a simple XOR operation or a more complex cryptographic function.

3. Equation for encryption

   Equation for encryption:

   - For the first plaintext bit, x_1, the encryption equation can be written as:

   $$y_1 = e(x_1 \oplus IV, k)$$

   Where $\oplus$ denotes the XOR operation.

   - For subsequent bits x_i (with $i > 1$):

   $$y_i = e(x_i \oplus y_{i-1}, k)$$

   Here, e is a function representing the encryption mechanism using the key k.

b. Decryption Equation
   i. The decryption process works similarly but in reverse, using the function e^-1 which is inverse of encryption equation
      1. Initial setup
         a. The decryption starts with the ciphertext y1, and uses the same key k to reverse the process.
      2. Equation for decryption

         For the first ciphertext y_1, the decryption equation is:

         $$x_1 = e^{-1}(y_1, k) \oplus IV$$

         For subsequent ciphertexts y_i (with $i > 1$):

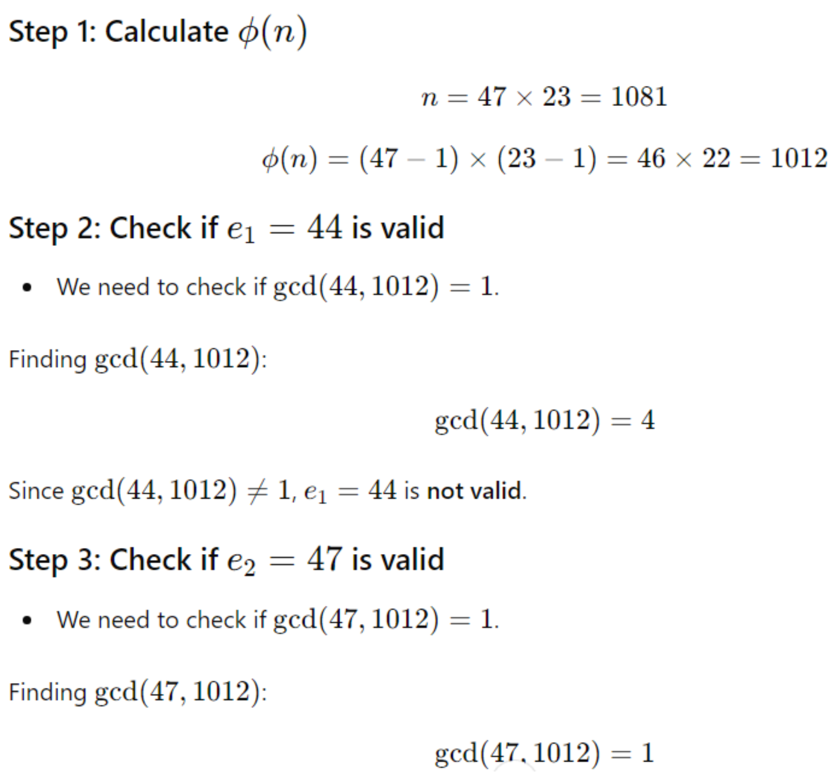
         $$x_i = e^{-1}(y_i, k) \oplus y_{i-1}$$

      3. This feedback mechanism allows both encryption and decryption to be performed iteratively. The use of yi in the encryption and decryption steps introduces diffusion, meaning that each bit of ciphertext is dependent not only on the corresponding plaintext bit but also on the previous ciphertext bit.

3. RSA

   Given:

   - p=47
   - q=23


Step 1: Calculate $\phi(n)$

$$n = 47 \times 23 = 1081$$

$$\phi(n) = (47 - 1) \times (23 - 1) = 46 \times 22 = 1012$$

Step 2: Check if $e_1 = 44$ is valid

- We need to check if $\gcd(44, 1012) = 1$.

Finding $\gcd(44, 1012)$:

$$\gcd(44, 1012) = 4$$

Since $\gcd(44, 1012) \neq 1$, $e_1 = 44$ is **not valid**.

Step 3: Check if $e_2 = 47$ is valid

- We need to check if $\gcd(47, 1012) = 1$.

Finding $\gcd(47, 1012)$:

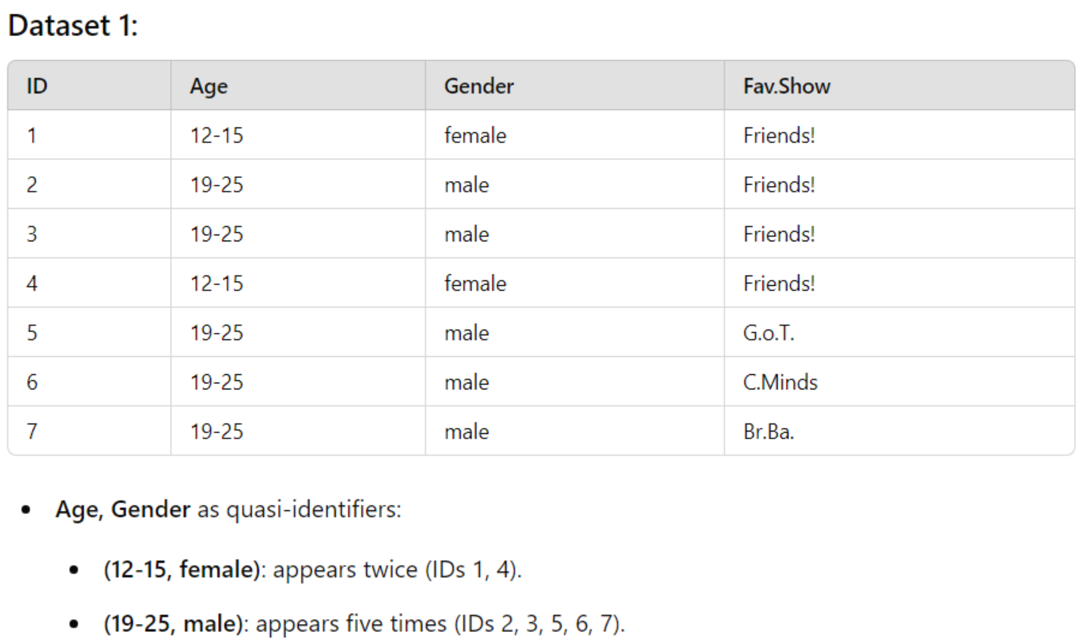
a. $$\gcd(47, 1012) = 1$$

b. Since gcd(47,1012)=1, e2 = 47 is **valid**.

Conclusion:

- e1=44 is not a valid RSA exponent.
- e2=4 is a valid RSA exponent because it is relatively prime to ϕ(n)=1012

4. K-Anonymity
   a. Quasi Identifiers in Datasets
      i. **ID**: This is a unique identifier and should not be considered in the quasi-identifiers for assessing anonymity.
      ii. **Age**: This could be considered as a quasi-identifier.
      iii. **Gender**: Another quasi-identifier.
      iv. **Favorite Show (Fav.Show)**: This attribute could be sensitive, but for now, we focus on **Age** and **Gender** as quasi-identifiers to assess anonymity.
      v. Analyze each dataset and find the maximum k for which k-anonymity is satisfied.



Dataset 1:

ID	Age	Gender	Fav.Show
1	12-15	female	Friends!
2	19-25	male	Friends!
3	19-25	male	Friends!
4	12-15	female	Friends!
5	19-25	male	G.o.T.
6	19-25	male	C.Minds
7	19-25	male	Br.Ba.

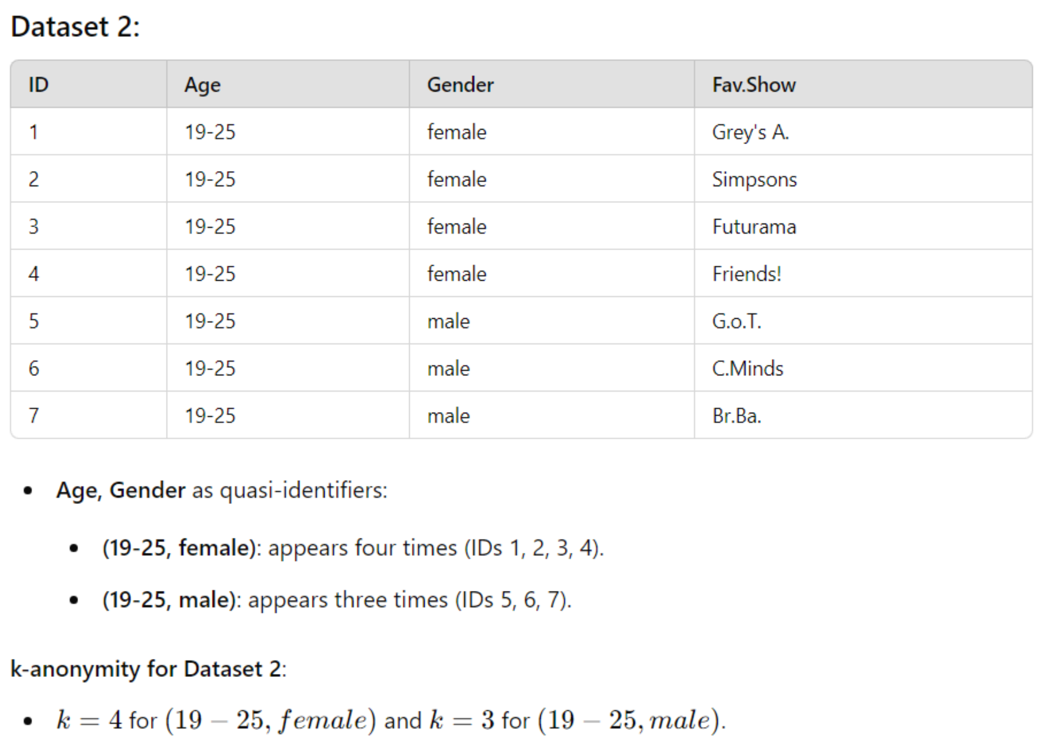
- **Age, Gender** as quasi-identifiers:
  - **(12-15, female)**: appears twice (IDs 1, 4).
  - **(19-25, male)**: appears five times (IDs 2, 3, 5, 6, 7).

b.

c. Age, Gender as quasi-identifiers:
   i. (12-15, female): appears twice (IDs 1, 4).
   ii. (19-25, male): appears five times (IDs 2, 3, 5, 6, 7).

k-anonymity for Dataset 1:

- The largest set of indistinguishable rows is based on (19−25,male)(19-25, male)(19−25,male), which appears 5 times.
- k=2k = 2k=2 for (12−15,female)(12-15, female)(12−15,female) and k=5k = 5k=5 for (19−25,male)(19-25, male)(19−25,male).
- The maximal k for Dataset 1 is **5** (since the largest anonymity set involves 5 rows).



Dataset 2:

ID	Age	Gender	Fav.Show
1	19-25	female	Grey's A.
2	19-25	female	Simpsons
3	19-25	female	Futurama
4	19-25	female	Friends!
5	19-25	male	G.o.T.
6	19-25	male	C.Minds
7	19-25	male	Br.Ba.

- **Age, Gender** as quasi-identifiers:
  - **(19-25, female)**: appears four times (IDs 1, 2, 3, 4).
  - **(19-25, male)**: appears three times (IDs 5, 6, 7).

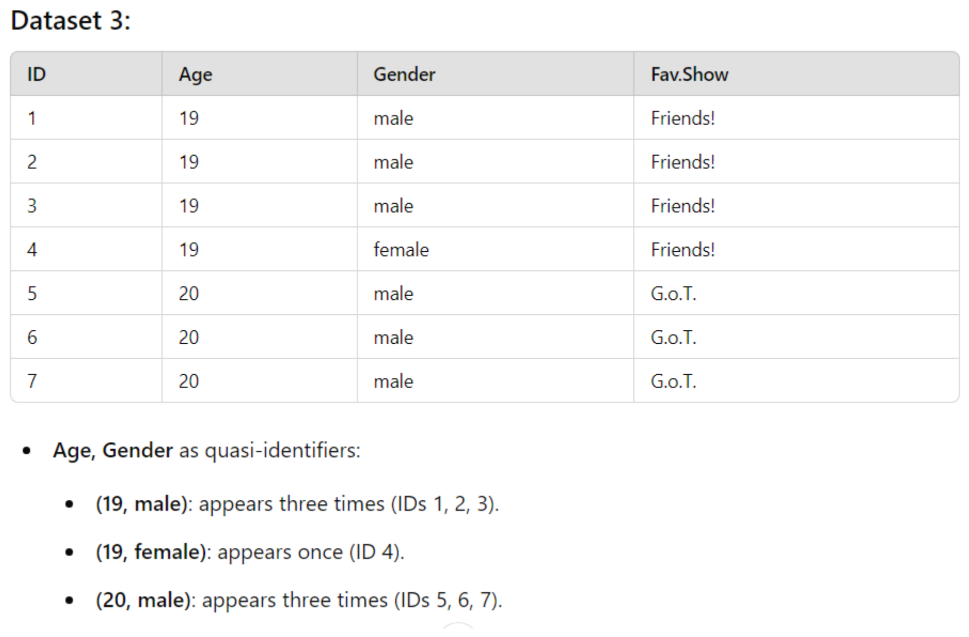
k-anonymity for Dataset 2:

- $k = 4$ for $(19 - 25, female)$ and $k = 3$ for $(19 - 25, male)$.

d.

k-anonymity for Dataset 2:

- k=4 for (19−25,female) and k=3 for (19−25,male)
  - The maximal k for Dataset 2 is **4**.



Dataset 3:

ID	Age	Gender	Fav.Show
1	19	male	Friends!
2	19	male	Friends!
3	19	male	Friends!
4	19	female	Friends!
5	20	male	G.o.T.
6	20	male	G.o.T.
7	20	male	G.o.T.

- **Age, Gender** as quasi-identifiers:
  - **(19, male)**: appears three times (IDs 1, 2, 3).
  - **(19, female)**: appears once (ID 4).
  - **(20, male)**: appears three times (IDs 5, 6, 7).

e.

k-anonymity for Dataset 3:

- k=3 for (19,male) and (20,male).

- k=1 for (19,female) (which means this does **not** satisfy 2-anonymity for this group).

Conclusion:

- **Dataset 1** satisfies **5-anonymity** (maximal k=5).
- **Dataset 2** satisfies **4-anonymity** (maximal k=4).
- **Dataset 3** satisfies **3-anonymity** for the male groups but does **not** satisfy 2-anonymity for all records due to the single occurrence of (19,female).

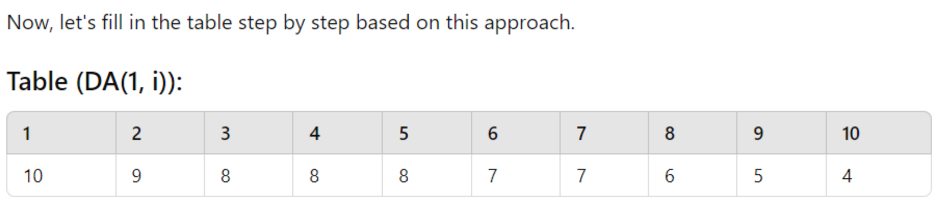
5. Moving P to Q
    a. To calculate the cost of moving set P to set Q, we need to define a cost metric. One common approach is to compute the **minimum distance** between corresponding elements in each set, typically using a metric such as the **Manhattan distance** or **Euclidean distance**.
    b. Given
        i. P={6k,8k,11k}
        ii. Q={3k,3k,5k,6k,7k,8k,9k,10k}
    c. Matching salaries from P to Q
        i. **Match 6k from P to the closest in Q**:
            1. Available in Q: 6k (exact match).
            2. Cost: 0
        ii. **Match 8k from PPP to the closest in QQQ**:
            - Available in QQQ: 8k8k8k (exact match).
            - Cost: 000.
        iii. **Match 11k from PPP to the closest in QQQ**:
            - Closest in Q: 10k (next highest available).
            - Cost: 11k − 10k = 1k.

Total Cost:

- 0 + 0 + 1K = 1K

        iv. Thus, the cost of moving P to Q is **1k**.
6. K-degree anonymity
    a. The given data is:
        i. 10,9,8,8,8,7,7,6,5,4
    b. We need to ensure that each value in the list has at least 3 occurrences that satisfy DA(1,i) ≥ k
    c. Steps
        i. The maximum degree for i=1 would be 10, because there are 10 values.

d.

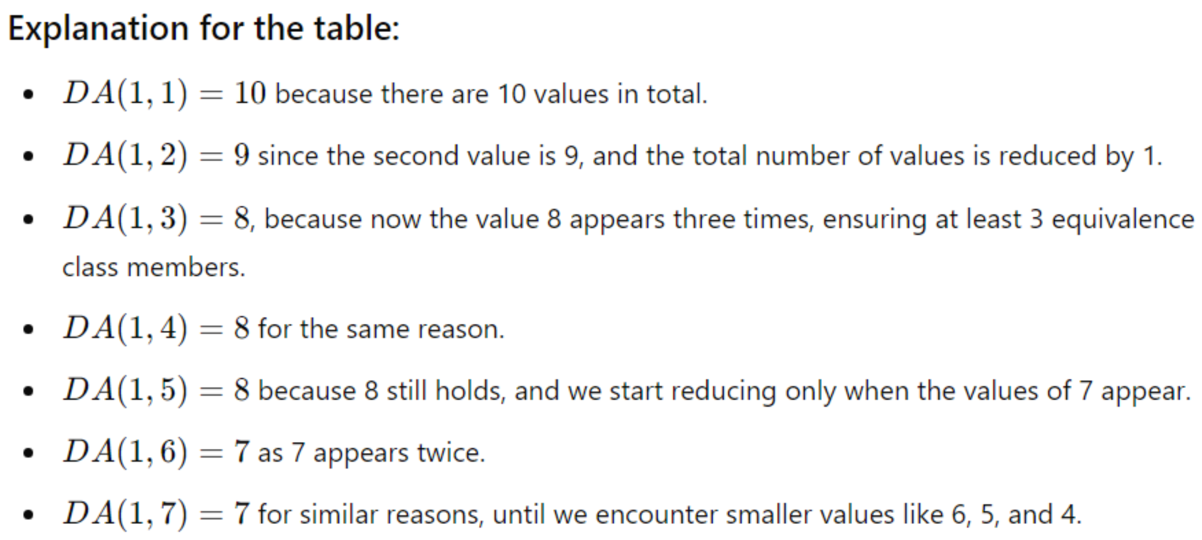


Now, let's fill in the table step by step based on this approach.

Table (DA(1, i)):

1	2	3	4	5	6	7	8	9	10
10	9	8	8	8	7	7	6	5	4

e.



Explanation for the table:

- $DA(1,1) = 10$ because there are 10 values in total.
- $DA(1,2) = 9$ since the second value is 9, and the total number of values is reduced by 1.
- $DA(1,3) = 8$, because now the value 8 appears three times, ensuring at least 3 equivalence class members.
- $DA(1,4) = 8$ for the same reason.
- $DA(1,5) = 8$ because 8 still holds, and we start reducing only when the values of 7 appear.
- $DA(1,6) = 7$ as 7 appears twice.
- $DA(1,7) = 7$ for similar reasons, until we encounter smaller values like 6, 5, and 4.