```
x = 2388 (for DOG):
i   | b_i |                           | z
---------------------------------------------
0   | 1   | 1^2 * 2388                | 2388
1   | 0   | 2388^2                    | 3578
2   | 0   | 3578^2                    | 26380
3   | 1   | 26380^2 * 2388            | 393
4   | 1   | 393^2 * 2388             | 19698
5   | 0   | 19698^2                   | 11821
6   | 0   | 11821^2                   | 17435
7   | 1   | 17435^2 * 2388           | 8167
8   | 1   | 8167^2 * 2388            | 30153
9   | 0   | 30153^2                   | 30454
10  | 0   | 30454^2                   | 17682
11  | 0   | 17682^2                   | 24132
12  | 1   | 24132^2 * 2388           | 15407
2388^4913 mod 31313 = 15407
```

```
x = 1371 (for CAT):
i   | b_i |                           | z
---------------------------------------------
0   | 1   | 1^2 * 1371                | 1371
1   | 0   | 1371^2                    | 861
2   | 0   | 861^2                     | 21122
3   | 1   | 21122^2 * 1371           | 10339
4   | 1   | 10339^2 * 1371           | 17937
5   | 0   | 17937^2                   | 26207
6   | 0   | 26207^2                   | 18820
7   | 1   | 18820^2 * 1371           | 3655
8   | 1   | 3655^2 * 1371            | 30384
9   | 0   | 30384^2                   | 17590
10  | 0   | 17590^2                   | 4347
11  | 0   | 4347^2                    | 14670
12  | 1   | 14670^2 * 1371           | 25076
1371^4913 mod 31313 = 25076
```