0 Argument

Assuming $|B| = 2^l$ and there are l functions $g_i(x) : \{0,1\}^{256} \to \{0,1\}$ $(0 \le i < l)$. If the probability that the output is 1 for a random x should be independent events, and for each function in this functional series, the probability that the output equals 1 is $\frac{1}{2}$, then F distributes A uniformly on B. In fact, these two statements are equivalent. This is important because it's known that each of these functions is undetectable individually, and we don't want to make them easier to detect when the hacker can query all l functions. When F has a uniform distribution, it's impossible for hackers to achieve a function like h where knowing some of the $g_i(x)$s can't guess an unknown $g_j(x)$ with an accuracy grater than $\frac{1}{2}$.

If in the second query, the hacker can find out $F(a)$ where $a \in$ cipher-text bank, we can use a bank with equal X_is (I suggest doing it for more security against known cipher-text attacks). X_i is the size of $bank[i]$, $i \in B$. Otherwise, it's necessary to achieve a good key that distributes A more uniformly. With numerical tests on g_i functions, it is possible to understand how far from ideal conditions we are, but it doesn't provide a certain quantity, so I offer these two tests.

1 Tail Test

In this test, the expected population of cell number 0 is examined in the ideal case (shown as $e(0)$) and for a particular key (shown as $e'(0)$). This utilizes the fact that with $1 < k$, an array $< a_i >$ of positive numbers with a fixed value of $\sum a_i$ has the minimum value of $\sum {a_i}^k$ when all a_is are equal.

$$I \sim GOORB(n,k)$$

$$e(0) = \frac{(n-1)^k}{n^{k-1}} = n\frac{(n-1)^k}{n^k} = nP^k, \; P = \frac{n-1}{n}$$

For a particular key, $e'(0)$ can be computed by summing the probability that b won't be chosen in any round after the k^{th} round, for all $b \in B$. It can be computed by experimental methods and can be displayed as nQ^k, $(0 < Q < 1)$, and since in each round exactly one element will be chosen, $\sum(1-p_i) = n-1$ holds for both cases (p_i is the probability that the i^{th} element will be chosen in a round).

$$e'(0) = \sum_{i=1}^{n}(1-p_i)^k = nQ^k$$

Now, it's known that $e(0) < e'(0)$, so a parameter named safety_rate is defined as below. When the safety rate is closer to 1, it means we achieved a safer key; otherwise:

$$nP^k \le nQ^k \to P^k \le Q^k$$

$$\text{safety\_rate} \in (0,1], \; \text{safety\_rate} = 1 - Q^k + P^k$$

2 Head Test

In this test, the maximum number of times a player has been selected in the ideal case and for a particular key are compared together. By utilizing the **Law of Large Numbers**, it's possible to approximate this quantity for the ideal case, and using experimental methods it's possible to approximate it for that particular key. [1]

$$E[max\{X_1, ..., X_n\}] = M \approx \frac{k}{n} + \sqrt{\frac{2k\ln(n)}{n}}$$
$$E[max\{X'_1, ..., X'_n\}] = M'$$

It's possible to prove that for big enough ks, always $M << M'$. Assume the greatest chance to be selected in a round is $\frac{q}{n}, (1 < q)$, so the expected value of being selected is $\frac{kq}{n} \leq M'$. And again, like the former test, a parameter is defined to measure how safe the key is:

$$\frac{k}{n} + \sqrt{\frac{2k\ln(n)}{n}} \leq \frac{kq}{n} \leq M' \leftrightarrow \sqrt{\frac{2k\ln(n)}{n}} \leq \frac{k(q-1)}{n}$$
$$\leftrightarrow \sqrt{2n\ln(n)} \leq \sqrt{k}(q-1) \leftrightarrow \frac{2n\ln(n)}{(q-1)^2} \leq k$$
$$\text{safety\_rate} \in (0,1], \ \text{safety\_rate} = 1 - \frac{M' - M}{k}$$

[1] For more info about the **Law of Large Numbers**:
https://ocw.mit.edu/courses/9-07-statistics-for-brain-and-cognitive-science-fall-2016/42505b2c837e6182a408650e242d9830_MIT9_07F16_lec7.pdf