• Random Oracle Model:

The random oracle model is an mathematical model for a hash function. A hash function based on this model behaves as follows,

i) When a new message of any length is given, the oracle model creates and gives a fixed length message digest. The oracle records the message and the message digest.

ii) When a message is given for which a digest exists, the oracle model simply gives the digest in the record.

iii) The digest for a new message needs to be chosen independently from all previous digest. That is the oracle cannot use a formula or an algorithm to calculate the digest.

Pigeonhole principle:

If n pigeonholes are occupied by n+1 pigeons, then atleast one pigeonhole is occupied by two pigeons.

The generalized version of the pegionhole principle is that if n pigeonholes are occupied by Kn+1 pigeons, then atleast one pigeonhole is occupied by K+1 pigeons.

Because the whole idea of hashing dictates that the digest should be shorter than the message, according to pigeonhole principle, there are some digests that

correspond to more than one message.

Example:

Assume that the messages in a hash function are 6 bits long and the digests are only 4 bits long. Then the possible number of digests (pigeonholes) is $2^4 = 16$ and the possible number of message (pegeon) is $2^6 = 64$. This means $n = 16$ and $Kn + 1 = 64$, so K is larger than 3. By pigeonhole principle the conclusion is that atleast one digest corresponds to four $(K+1)$ messages.

Birthday problem:

The second thing we need to know for analyzing the random oracle model is the famous birthday problem.

problem 1:

What is the minimum number, K of the students in a classroom such that it is likely that atleast one student has a predefined birthday?

This problem can be generalized as follows. ~~that~~ we have an uniformly distributed random variable with N possible values. What is the minimum number of instances, K, such that it is likely that at least one instance is equal to a predefined value?

Problem 2:

what is the minimum number k of students in a classroom such that it is likely that atleast one student has the same birthday as the student selected by the professor?

Problem 3:

What is the minimum number k of students in a classroom such that it is likely that at least two students have the same birthday.

Problem 4:

We have two classes, each with k students. What is the minimum value of k so that it is likely that atleast one student from the first classroom has the same birthday as a student from the second classroom.

The summarized solutions to the four birthday problems:

Problem	Probability	General value for k	Value of k with $P=1/2$	Number of students ($N=365$)
1	$P=1-e^{-k/N}$	$K=\ln[1/(1-P)]\times N$	$K=0.69\times N$	253
2	$P=1-e^{-(k-1)/N}$	$K=\ln[1/(1-P)]\times N+1$	$K=0.69\times N+1$	254
3	$P=1-e^{k(k-1)/2N}$	$K=\{2\ln[1/(1-P)]\}^{1/2}\times N^{1/2}$	$K=1.18\times N^{1/2}$	23
4	$P=1-e^{-k^2/2N}$	$K=\{\ln[1/(1-P)]\}^{1/2}\times N^{1/2}$	$K=0.83\times N^{1/2}$	16

The value 23 is the solution to the classical birthday paradox. If there are just 23 in a classroom, it is likely (with $P \geq 12$) that two students have the same birthday (ignoring the year they have been born).

Attacks on Random Oracle Model:

Preimage attack:

To find the probability we use the first birthday problem. The probability of success is $P = 1 - e^{-K/N}$

If Eve needs to be 50% successful, what should be the size of K?

We know,

$$K = 0.69 \times N$$

or $K = 0.69 \times 2^n$

In other words, for Eve to be successful more than 50% of time, she needs to create a list of digest that proportional to 2^n

Note: The difficulty of a preimage attack is proportional to 2^n

Example:

A cryptographic hash function uses a digest of 64 bits. How many digests does Eve need to create to find the original message with the probability more than 0.5?

Sol^n

The number of digest that can be created is,

$$K = 0.69 \times 2^{64} \quad \text{(This is fairly large enough)}$$

Even if Eve can create 2^{30} (almost a billion) per second. it takes 0.69×2^{34} seconds or more than 500 years.

This means that a message digest of size 64 bits is Secure with respect to preimage attack.

Second Preimage Attack:

To find the probability, we use the second birthday problem. The probability of success is

$$P = 1 - e^{-(K-1)/N}$$

If Eve needs to be at least 50% successful, what should be the size of K.?

we know by second type birthday problem

$$K = 0.69 \times N + 1$$

$$\text{or } K = 0.69 \times 2^n + 1$$

In other words for Eve to be successful more than 50% of the time, she needs to create a list of digest that is proportional to 2^n.

Note: The difficulty of a Second preimage is proportional to 2^n

Collision Attack:

To find the probability we use the third birthday problem. The probability of success is

$P = 1 - e^{-K(K-1)/2N}$

If Eve needs to ~~find~~ be at least 50% successful what should be the size of K?

we know from third birthday problem,

$$K = 1.18 \times N^{1/2}$$

$$\Rightarrow K = 1.18 \times 2^{n/2}$$

In other words for Eve to be successful more than 50 percent of time, she needs to create a list of digest that is proportional to $2^{n/2}$

Note: The difficulty of a collision attack is proportional to $2^{n/2}$

Example:

A cryptographic hash function uses a digest of 64 bits. How many digests does Eve needs to create to find two messages with the same digest with the probability more than 0.5?

Soln

The number of digest to be created is,

$$K = 1.18 \times 2^{n/2}$$

$$\therefore K = 1.18 \times 2^{32}$$

If Eve can test 2^{20} (almost one million) messages per second, it takes 1.18×2^{12} seconds or less than two hours. This means that a message digest of size 64 bits is not secure against the collision attack.

Alternate Collision Attack:

To find the probability we use the fourth birthday problem. The probability of success is $P = 1 - e^{-K^2/N}$

If Eve needs to be atleast 50% successful, what should be the size of K?

We know by fourth birthday problem,

$$K = 0.83 \times N^{1/2}$$

$$\therefore K = 0.83 \times 2^{n/2}$$

In other word for Eve to be successful more than 50% of times, she needs to create a list of digests that is proportional to $2^{n/2}$

Note: The difficulty of an alternative collision attack is proportional to 2^n