RNG stands for ‘Random Number Generator’. In machine aided gambling, it sets the odds for an outcome in a game. Most of the methods start with a ‘seed’ or number. This is fed into a procedure to generate the next number and so on depending on the algorithm used. Unfortunately, if you use the same seed number, you will always generate the same sequence of numbers since procedural code does not change. That is why the term ‘random’ is a misnomer in a computer chip based RNG. There are ways to make the seed randomly generated and briefly explained at the end of this article.

Video Slot Machines, RNG and PRNG

In a video gaming machine, RNG is a function (set of procedures in computer code) stored on an EPROM chip. Its purpose is to create random numbers within a defined range for example, zero to one million. Another function performs a division on the random number creating a remainder. This process is used to determine for example, in displaying a reel’ position in a slot machine. Each RNG is independent of a previously generated RNG although this may seem counterintuitive since using the same seed will each time produce the same set of RNG numbers.

Video gambling machines use PRNG chips, (pseudo-random number generator). The trick is that the random number generator code produces a list of millions of random numbers, before repeating the sequence. These random number lists are either generated periodically or at set intervals. The amount of memory available in the chips set of the machine usually dictates the list length and the regeneration interval. There may be several PRNGs, acting together or under control of a master chip. While such lists are inadequate for cryptography, they work well enough for online and slot machine gaming.

One misconception is that idle machines are in a wait or holding pattern until a play is generated. In fact, the RNG function may operate continuously until the machine is powered down, all the time creating new numbers. This implies that winning combinations occur continuously but are not displayed while a machine is idle. Players who think that a machine will be hot because a previous player did not win are working under a misconception.

Another misconception is that the PRNG is affected by game actions and events such as length of play, amount of bet, use of a reward card, strategy or choices. The RNG simply creates numbers that pass a statistical test of repeatability.

A PRNG does not need to start with an actual seed number from a finite list. Some systems use physical devices, physical activity and other measurements that are unrelated as input into a seed generator logic. This principle is based on the concept of entropy where it is difficult to reproduce or predict an exact state that can be used to create a starting seed for the PRNG algorithm. In computers for example, it may use things like noise1, thermal characteristics, network and CPU activity, and other events that a computer can monitor and use in an entropy seed calculation. While these may not satisfy the ‘true random statistical test’, they do satisfy the condition of unpredictability in a given time unit.

1 One online casino ‘talks to the stars’ capturing noise in space for its server seed generator logic.
Random Number Generators in Gambling

A second seed step may use other statistical methods that are classified as ‘stochastic’. In a stochastic or random process there is some unpredictability in the next outcome that follows some probability distribution.

So, even with the same starting seed number, a process may choose different outcomes with some more probable than others. While these random numbers are independent per unit of time, they are however, statistically correlated. A typical test (image left) analyzes across two dimensions (X,Y) over time (Z).

Online Video Card Gambling PRNG

Here is how one online video card gambling site creates random numbers.

Our approach is to take seeds from that pool on a periodic basis. These seeds serve as the starting number for an elementary cellular automaton. A cellular automaton in our case is an array of binary values. A complex rule for state transitions creates new random numbers from the seed value. We use a rule known to produce randomness. "Rule 30 is of special interest because it is chaotic ... this rule is used as the random number generator used for large integers in Mathematica."

Once we have that seed, we produce random number through the state transitions of the cellular automaton. Our cellular automaton has 256 bits. We take the additional step of randomly selecting one (1) bit from each of the successive 255 rows (states) to produce our random numbers.

Our random number generator passed two (2) standard tests: the Diehard and the ENT tests. More importantly, we our code has been inspected and certified by an independent testing lab specializing in the analysis, review, and certification of software for gaming and cryptology.

A random number generator is only part of the story in producing randomly distributed decks of cards. How the deck is shuffled is equally important. We have selected an algorithm (process) that ensures a true randomizing shuffle. This approach does not favor any one card or any one position in the deck.

We then assign each card a 256 bit random number. This very large number is greater than 1 with 77 zeros after it. With each card given its own huge random number, we sort the deck by those random numbers, placing the cards in yet another random sequence. This algorithm also ensures that every possible card sequence is theoretically equally likely to occur.

Our approach relies on well-accepted random number generation tools, relying on system entropy to generate random seeds. We then use a system known to generate randomly distributed numbers from the seed number. As a further security step, we periodically select a new seed. Our decks are randomized prior to first use, and then serve as the random base from which a randomizing shuffle is applied. (www.5betpoker.com)
Random Number Generators in Gambling

Payout and the concepts of ‘loose’ and ‘tight’

A PRNG is part of an instruction set that determines the outcome of a game. The outcome is governed by a set of parameters (game rules, bet rules and outcome rules). The combination of rules can be adjusted to produce different predictable outcomes that fall between limits defined as being loose and tight.

These are not statistical terms but simply mean that an outcome with a favorable result (payoff) will occur more frequently under loose conditions than under tight conditions. In mathematical terms this is referred to as volatility, namely how often or not favorable outcomes occur per unit of time.

This may be complicated to predict because parameters can be set to have higher or lower volatility in short intervals versus long intervals. This means that a player may have more or favorable outcomes in short intervals followed by less favorable outcomes in longer intervals and vice versa. That’s why the term ‘loose slots’ may mean different things depending on the length of play.

Up to now, video slot machines were quasi-independent from a central control. A video game odds are dictated by how the game parameters are set (loose or tight) and the theoretical win (theo) of the game whose random numbers are generated by the PRNG chip. Once set, this machine produces, on average over the long run, the expected payout percentage. A loose machine could return 97 percent and a tight machine 92 percent.

However, the newer generation of video machines are managed and somewhat controlled by a central server. This allows casinos to change the displayed game periodically based on traffic patterns and games played in different parts of the floor. While the PRNG generators in a machine remain unchanged, the game type can change. That favorite loose game of yours in one machine location, is no longer loose in another machine location.

State laws define how RNGs are certified and how they statistically perform. An RNG must meet the expectation of a certain frequency of positive outcome (wins) over time. This defines the theoretical win or ‘theo’. In Nevada for example, slot machines have to pay back no less than 75 percent of what is bet (put into the machine) over time. PRNG chips are usually part of a processing chip set that is mechanically sealed, numbered and tracked in a database. Replacement of chips is governed by different state rules but random inspection is a common compliance rule.

Yes Alice, there is randomness but not like you think. What looks like chance can repeat itself and what repeats may not happen again.

“All things must end or change” – Leo Tolstoy.