



Random Bit Generator Theory of Operation

The noise in the Zener is loudest when the current through the zener is around 10uA
 So: 0V ground + .75V Base-Emitter voltage on 2n3904 = .75V
 $.75V + 1.22V$ across Zener = 1.97V
 $(3V - 1.97V) = 1.03V$ across 100K R1, so 10.3uA, good enough
 $10.3uA * \sim 200$ Current Gain (Hfe) = 2mA
 $3V - (2mA * 470R) = 1.59V$, close to the middle of the 3V Vcc
 Zener current is noisy, that noise is amplified by 2n3904 too
 And due to cap, only this noise is taken and sent to the op amp
 Amp has an extremely large gain, due to 1M ohm feedback resistor.
 For good measure, the signal is fed through a second op amp acting as a comparator.
 This is fed as a digital signal into the atmega8
 The Atmega8 has a timer ISR that triggers every 32uS, sampling the digital input
 The Von Neumann Method is implemented in this ISR to de-bias the input
 When the conditions of the method are met, the new bit is mixed into a 32 bit number
 Hence, this 32 bit number is both random and constantly updated



open hardware

Random bit generator hardware from Leon Nathaniel Maurer, <http://tinyurl.com/DIYrandomgen>

Multi-Sized dice roller

CC BY-SA Harry Johnson github.com/hjohnson

TITLE: D&D_dice_1

Document Number:

REV:

Date: 3/26/12 10:17 AM

Sheet: 1/1