True Random Generator (companion code for circuit)

This function will generate a true random number from the Random Bit Generator for cryptographic strength random numbers circuit.

An upper limit and resolution must be specified. The higher the resolution the longer time required to return a value but the less “course” the answer. e.g. if you specify a maximum of 100 with a resolution of 4 bits (2^4=16), the smallest value that can be returned is 6.25 (100/16), whereas a resolution of 16 (2^16=65536) will return a minimum resolution of 0.0015259 (100/65536). Choose a value which is a good compromise of resolution versus speed.

Syntax: TRnd!(Upper_Limit,Resolution)

Resolution is

```
1 < x < 64
```

bits Return is

```
0 <= x < Upper_Limit
```

Example: t!=TRnd!(100,16)

Maths Considerations:

With the default single precision floating point of the MicroMite, a practical limit of 18 bits should be observed. More than this results in the rounding errors of the maths pack becoming a significant contributor to the returned value. e.g. by holding the input pin high (to force a maximum count)

```
TRnd!(2,18)
```

returns

```
1.99999
```

But

```
TRnd!(2,19)
```

returns

```
2
```

which clearly breaks the rule of x < Upper_Limit

The double precision of MMX MMBasic will push this limit out further but is moot as the RND() function uses the TRNG generator of the PIC32MZ.

Assumptions:

```
   SETPIN 1,DIN
```

Code:

```
    FUNCTION TRnd!(x AS FLOAT,bits AS INTEGER)
      LOCAL INTEGER n,t,b
      b=Max(Min(bits,63),1) ' constrain bits to 1-63

      FOR n=1 TO b
        t=(t<<1) + PIN(1)
      NEXT

      TRnd!=(1/(2^b)*t)*x   ' the returned value can never be x but might be very close

    END FUNCTION
```