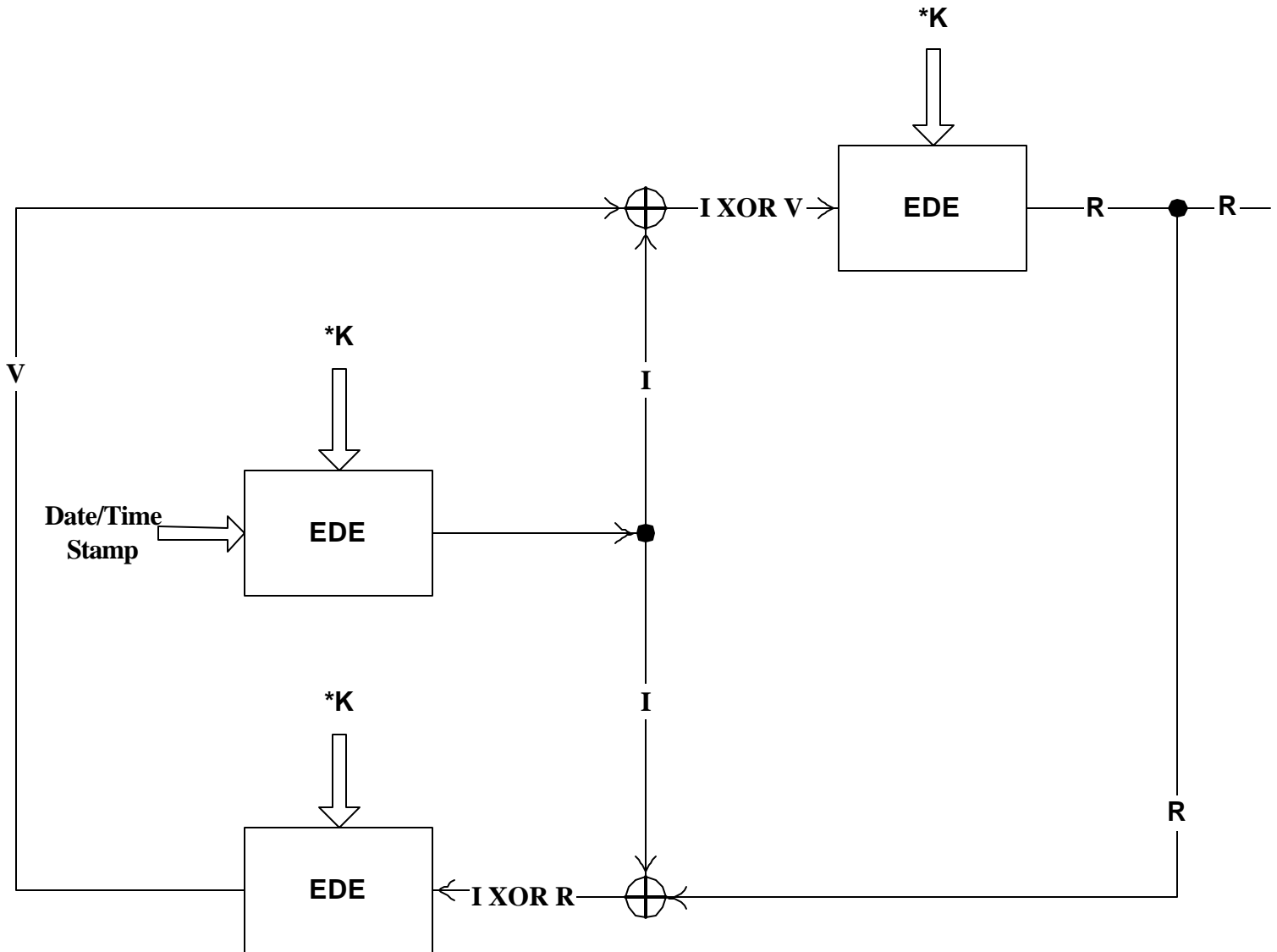


## The ANSI X9.31-1998 Appendix A.2.4 PRNG



### ANSI X9.31-1998 - Appendix A.2.4:

Let  $\text{ede}^*K(Y)$  represent the DEA multiple encryption of  $Y$  under the key  $*K$ . Let  $*K$  be a DEA key pair reserved only for the generation of pseudo random numbers, let  $V$  be a 64-bit seed value which is also kept secret, and let  $\wedge$  be the exclusive-or operator. Let  $DT$  be a date/time vector which is updated on each iteration.  $I$  is an intermediate value. A 64 bit vector  $R$  is generated as follows:

$$I = \text{ede}^*K(DT)$$

$$R = \text{ede}^*K(I \wedge V) \text{ and a new } V \text{ is generated by } V = \text{ede}^*K(R \wedge I).$$

Successive values of  $R$  may be concatenated to produce a pseudo random number of the desired length.