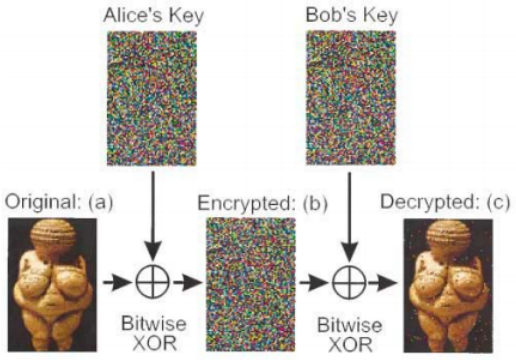
8.93: Coding and Decoding Venus

In 2000 Anton Zeilinger and his research team sent an encrypted photo of the fertility goddess Venus of Willendorf from Alice to Bob, two computers in two buildings about 400 meters apart. The figure summarizing this achievement first appeared in *Physical Review Letters* and later in a review article in *Nature*.



It is easy to produce a rudimentary simulation of the experiment. Bitwise XOR is nothing more than addition modulo 2. The original Venus and the shared key are represented by the following matrices, where the matrix elements are pixels that are either off (0) or on (1).

$$i = 1..7 \quad j = 1..6 \quad \mathrm{Key}_{i,j} = \mathrm{trunc}(\mathrm{rnd}(2)) \quad \mathrm{Key} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \mathrm{Venus} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

A coded version of Venus is prepared by adding Venus and the Key modulo 2 and sent to Bob.

$$\mathrm{CVenus}_{i,j} = \mathrm{Venus}_{i,j} \oplus \mathrm{Key}_{i,j} \quad \mathrm{CVenus} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Bob adds the key to CVenus modulo 2 and sends the result to his printer.

$$\mathrm{DVenus}_{i,j} = \mathrm{CVenus}_{i,j} \oplus \mathrm{Key}_{i,j} \quad \mathrm{DVenus} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

A graphic summary of the simulation: