



Problem 6. «A binary tape»

A cipher machine works with a binary infinite tape that starts with an input word of length n and all its other elements are zero. The machine encrypts an input word and writes the result instead of it.

The cipher machine can do two operations:

- 1) copy any symbol of the tape to other position;
- 2) apply some fixed one-to-one function $S : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ to the first m symbols, where $\mathbb{F}_2 = \{0, 1\}$.

Find the conditions for S such that the machine can perform any bijective mapping of words of length n .

Examples of operations.

- 1) For instance, the machine can copy the third symbol to the fifth place:

1	1	1	0	0	0	1	1	1	...
---	---	---	---	---	---	---	---	---	-----

the result will be

1	1	1	0	1	0	1	1	1	...
---	---	---	---	---	---	---	---	---	-----

- 2) Let m be 3 and $S(x, y, z) = (x, y, x \oplus z)$; applying S to the first three symbols:

1	1	1	0	0	0	1	1	1	...
---	---	---	---	---	---	---	---	---	-----

the result will be

1	1	0	0	0	0	1	1	1	...
---	---	---	---	---	---	---	---	---	-----