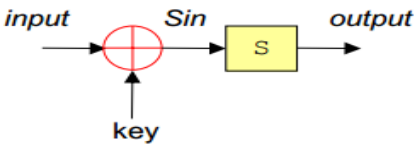
作业 a：回答：密码法哪一条款规定了，关键基础设施需要使用密码技术进行保护。

答：第二十七条:法律、行政法规和国家有关规定要求使用商用密码进行保护的**关键信息基础设施**，其运营者应当使用商用密码进行保护。

第三十七条:**关键信息基础设施**的运营者违反本法第二十七条第一款规定，由密码管理部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十方元以下罚款。

第三十七条:**关键信息基础设施**的运营者违反本法第二十七条第二款规定，由有关主管部门责令停止使用产品或服务，处采购金额一倍以上十倍以下罚款;对直接负责的主管人员和其他直接责任人一万元以上十万元以下罚款。

作业 b：结合差分功耗分析的原理，完成下面密钥恢复。



input		Sin	Sbox		output	power
			in	out		
00		?	00	01	?	2
01	Key =?	?	01	10	?	0
10		?	10	11	?	1
11		?	11	00	?	1

答：使用汉明重量的功耗模型，输出中 1 的数量代表功耗的大小,如果 power 为 1，则输出为 01 或 10,，powr 为 2 则输出为 11，据此反推出 Sin，猜测 key 的取值，与 input 作比较即可，通过比较得到下表：

Input	key	Sin	output	power
00	10	10	11	2

01	10	11	00	0
10	10/11	00/01	01/10	1
11	10/11	01/00	10/01	1

综上，可以得出 key 为 **10.**