2025-2026 年度广东省职业院校技能大赛
嵌入式系统应用开发赛项

竞赛任务书

（第四套）

竞赛注意事项

1. 选手竞赛过程中，各参赛选手应注意设备用电安全，禁止带电插拔设备的组件和模块，且务必远离饮用水、饮料等液体。若因操作不当导致设备出现问题应及时向现场裁判报告，由现场裁判处理。

2. 竞赛期间选手不得影响他人，干扰其他参赛选手的正常竞赛。

3. 所有参赛选手进入赛场后，直到竞赛结束之前，禁止向赛场任何人透露任何关于个人身份的相关信息。竞赛结束前需参赛选手签字确认的所有文件，只填写竞赛当天的工位号，填写其他信息均无效。

4. 参赛选手要注意及时保存电脑资料，由于操作不当导致文件丢失、损坏的，由参赛选手自行负责。

5. 选手可以在竞赛测试阶段的规定时间内按序进入练习赛道进行测试，每次限时 5 分钟，参赛队若放弃赛道任务测试机会，队长须前往竞赛测试区确认签字，表明自愿放弃测试机会，此次测试时间轮空且放弃不补，须等待下一轮测试机会，每队测试机会均等。

6. 第一模块竞赛共有两次测评机会，每次测评时长不超过 5 分钟，超过部分将不记录成绩。取两次中最高成绩为最终成绩，竞赛平台开始运行后需完全独立完成竞赛任务，期间不得手动控制，在竞赛平台启动之后，至选手确认竞赛测试结束之前，选手不得触碰竞赛平台。

7. 第二模块为综合展示，由各参赛队 1 名或多名队员根据第一个模块的竞赛内容和竞赛过程进行展示和讲解，所有参赛队统一不使用 PPT，限时 10 分钟。

8. 竞赛结束后，参赛选手应将现场下发所有资料、附件、资料盘等整理并交给现场裁判，不得将现场下发的任何材料带离竞赛现场。

比赛任务标志物摆放位置表

序号	设备名称	坐标点	说明
1	多功能信息显示标志物（A）	G3	朝向 F4
2	智能道闸标志物	E5	E4(道闸条位置)
3	智能交通信号灯标志物（A）	C3	C2（信号灯位置）
4	静态标志物（直）	C5	朝向 B5
5	智能 ETC 系统标志物	E2	朝向 B6
6	智能路灯标志物	G6	朝向 F6
7	立体显示标志物	A3	-
8	多功能信息显示标志物（B）	B7	朝向 B6
9	特殊地形标志物	E6	放置于 E6 坐标点 六张地形任意一张
10	智能显示标志物	D7	朝向 D6
11	智能无线充电标志物	B1	——
12	智能报警台标志物	E3	朝向 D2
13	智能交通交通灯标志物（B）	G5	F5（信号灯位置）
14	静态标志物（斜）	E7	朝向 F6
15	智能立体车库标志物（A）	D1	朝向 D2
16	竞赛平台（A）出发点	A4	-
17	竞赛平台（B）出发点	F7	-
18	RFID 卡片 (3 张)	RFID 卡片随机出现在 B6 至 F4 路段。	

比赛任务流程表

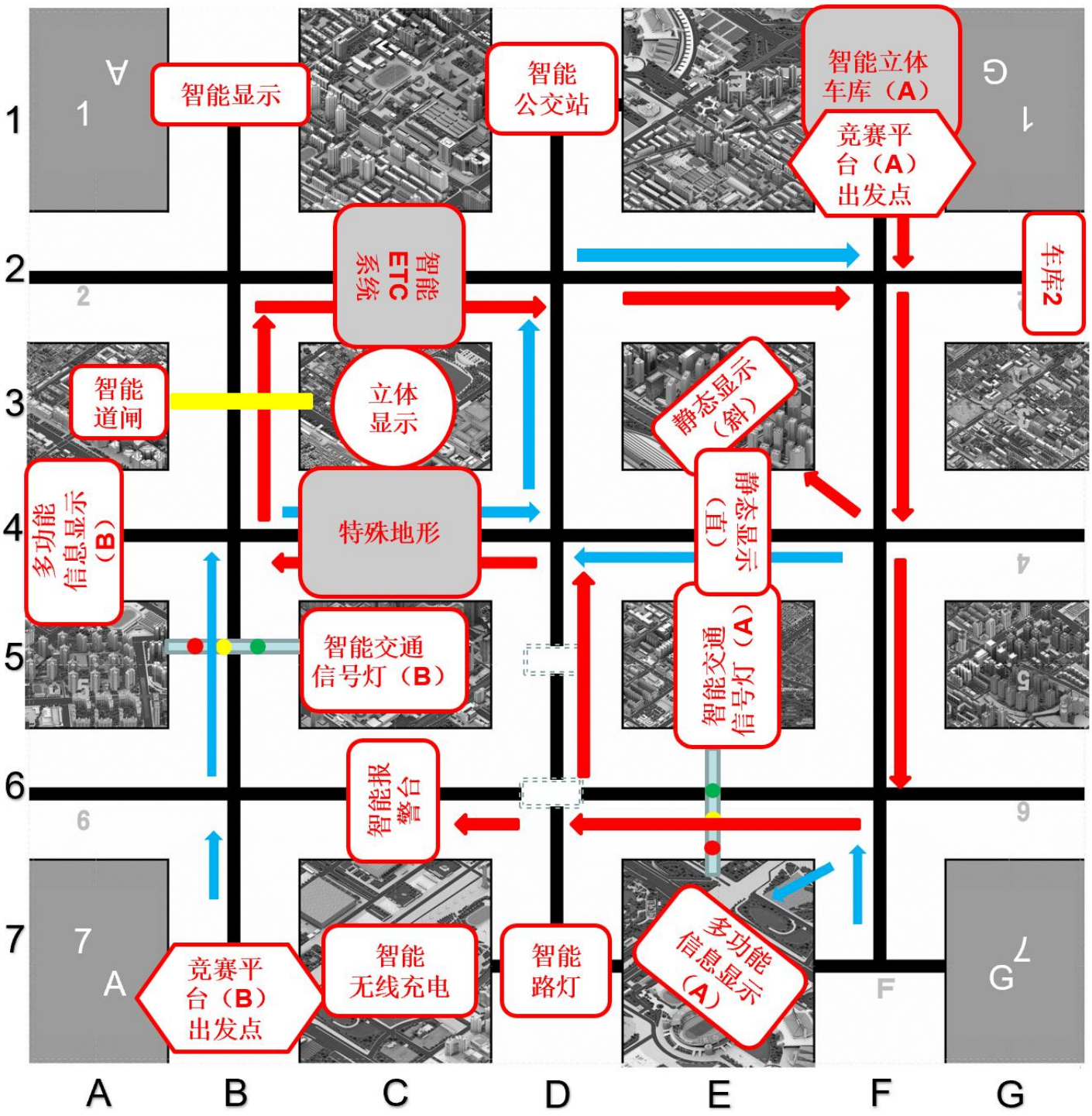
序号	任务要求	说明
1	竞赛平台（A）按以下指定路线行驶： F1→F2→F4→F6→D6→D4→B4→B2→D2→F2→车库，竞赛平台（A）应全自动完成路线行驶及赛道任务。	1、竞赛平台（A）启动后，必须在5分钟内完成所有任务，超时后任务不得分。 2、竞赛平台（A）应全自动完成所有任务与路径动作，期间不得通过任何形式触碰和干扰设备（裁判长对此拥有最终解释权与决策权）。 3、竞赛平台（A）需按照指定路线行驶，脱离指定路线外任务不得分。
2	任务一：竞赛平台（A）启动出库任务 竞赛平台（A）控制智能显示标志物进入计时状态，竞赛平台（A）顺利出库。	1、智能显示标志物进入计时状态后，竞赛平台（A）方可出库。
3	任务二：竞赛平台（A）距离探测任务 竞赛平台（A）由F2行进至F4位置处，向位于E4处的静态标志物A（直）进行测距，获得距离信息。	1、信息代码M01：超声波测距值（范围：100-400mm）。 2、超声波测距任务中测距起点为F4中心点，测距终点为静态标志物A（直）表面，误差范围±20mm。 3.将所测距离信息发送至智能显示标志物第二排以距离显示模式显示。
4	任务三：竞赛平台（A）二维码识别 竞赛平台（A）行进至F4位置处,扫描位于E3处静态标志物（斜）的二维码，并识别提取二维码中的有效信息。按要求获取有效信息后通过加密算法计算获得智能报警台标志物的6个字节红外开启码。	1、静态标志物（B）共存在2个二维码。2个二维码有效信息均存放于“<>”内，有效数据长度不固定，但在二维码可存储的有效长度内，有效数据长度较长的二维码为“二维码（1）”，有效数据长度较短的二维码为“二维码（2）”，需提取二维码（1）和二维码（2）中的有效数据带入数据处理算法后，解密得到报警台开启码，加密算法详见附件。 例：二维码（1）信息：128*<0BCA8B4BEED9F7E0DF85F1A450BCE9A8>，则有效数据为0BCA8B4BEED9F7E0DF85F1A450BCE9A8。 二维码（2）信息：31<makelife>，则有效数据为makelife。
5	任务四：竞赛平台（A）图形识别任务 竞赛平台（A）由F4行进至F6位置处，控制位于E7处的多功能信息显示标志物（A）中图片翻页找到有效图片进行识别，并将图形信息(信息代码M02)按照指定格式发送到多功能信息显示标志物（A）(HEX显示模式）显示，将颜色信息(信息代码M03)按照指定格式发送到智能立体显示标志物（自定义文本累加显示模式）显示。	1、信息代码M02：多功能信息显示标志物（A）中显示的图形信息。 2、信息代码M03：多功能信息显示标志物（A）中显示的颜色信息。 3、多功能信息显示标志物A复位后显示一张默认图片，选手需要执行翻页操作找到需要识别的有效图片，有效图片为包含直行交通标识的图片，其他为无效图片。 4、图形类别统计信息格式：BbDdEe，其中，A代表矩形，a为矩形的数量（0~9）。B代表圆形，b为圆形的数量（0~9）。C代表三角形，c为三角形的数量（0~9）。D代表菱形，d为菱形数量（0~9）。E代表五角星，e为五角星数量（0~9）。此处规定正方形只归属于矩形，不归属于菱形，如果图形图片中有图形重叠时，只需统计完整图形，不统计被遮盖图形（下面颜色统计规则一致）。多功能信息显示标志物（A）显示图形信息格式（HEX显示模式）为BbDdEe。 例：圆形数量为2、菱形数量为3、五角星数量为4，则智能TFT显示标志物（A）上显示“B2D3E4”。 1、颜色信息格式：FrFgFbFy，其中，F为固定字符，r为红色图形数量（0~9）；g为绿色图形的数量（0~9）；b为蓝色图形的数量（0~9）;y为黄色图形的数量（0~9）。立体显示标志物显示格式为FrFgFbFy。

		例：红色图形数量为 1、绿色图形数量为 2、蓝色图形数量为 3、黄色图形数量为 4，则智能立体显示标志物显示“F1F2F3F4”。
6	任务五：竞赛平台（A）交通灯识别任务 竞赛平台（A）位于 F6 位置处，启动 E5 处的智能交通灯标志物（A）进入 10s 倒计时显示模式，竞赛平台（A）在规定时间内识别出当前智能交通灯标志物(A)显示的信号灯颜色，并将识别结果发送至智能交通灯标志物(A)。	1、竞赛平台（A）应在规定的时间内识别出交通灯信号颜色，并将识别结果按照指定格式发送至智能交通灯标志物(A)，超时结果无效。 2、竞赛平台（A）识别后只需将结果返回至智能交通灯标志物(A)即可，无需执行其他操作。
7	任务六：竞赛平台（A）智能路灯感知调节任务 竞赛平台（A）由 F6 行进至 D6 位置处，获取位于 D7 处的智能路灯标志物初始档位信息，并通过公式计算出智能路灯目标档位信息，最终控制智能路灯标志物调节至目标档位。	1、信息代码 M04：智能路灯标志物初始挡位值（范围 1-4）。 2、目标挡位 T 由路灯初始档位 M04 进行 T =（M04^3+3）%4+1 计算后得到。（^指代幂次方） 3、智能路灯若没有受到任何指令控制，则该任务不得分。
8	任务七：竞赛平台（A）开启烽火台 竞赛平台（A）位于 D6 位置处，发送指定格式指令控制位于 C6 处的智能报警台标志物进入报警状态。	1、信息代码 M05：智能报警台标志物开启码 2、智能报警台标志物开启码由任务三中获取二维码信息，经过数据处理算法运算之后得到。数据处理过程请参考数据处理算法文件。
9	任务八：竞赛平台（A）RFID 数据获取任务 竞赛平台（A）在从 F6->D6->D4 路线行进路径中存在两张 RFID 卡，竞赛平台（A）需进行寻卡，并读取有效 RFID 卡片有效数据块的信息。	1、RFID 卡数量共有 2 张，随机放置在 F6->D6->D4 路段的轨迹线上(包括坐标点)，且不与特殊地形接触。数据读取仅需验证 A 密钥即可。两张卡依据 4 扇区第 1 数据块中数据来区分。存放数据含有“ID01”的为卡 1,存放数据含有“ID02”的为卡 2。（注：RFID 中存放的数据格式均为字符对应的 ASCII 码，如字符“I”对应的存放数据为 0x49）。 2、卡 1 有效信息存放于 3 扇区中第 2 个数据块，卡二为无效卡。读取数据仅需验证 A 密钥即可。卡 1 内有效数据内容由字母‘A-Z’和数字‘1-4’构成，剔除英文字符，保留数字得出有效数据 M06。 例：卡中读出数据为“A1B2C3D4”，则有效数据：M06=1234。
10	任务九：竞赛平台（A）通过特殊地形任务 竞赛平台（A）由 D4 至 B4 行进路径中存在特殊地形标志物，竞赛平台（A）行进过程中禁止与特殊地形标志物两侧掩体发生碰撞。	1、特殊地形标志物放置位置为 C4 坐标点。 2、特殊地形标志物共计 6 张特殊地形卡片，练习赛道可任意更换，测评赛道卡片由裁判现场指定，选手不可更换。 3、运行过程中竞赛平台（A）未通过特殊地形标志物不得分。
11	任务十：竞赛平台（A）车牌、车型识别任务 竞赛平台（A）行至 B4 位置处，识别多功能信息显示标志物（B）中的车牌信息。	1、信息代码 M07：多功能信息显示标志物（B）中有效车牌信息。 2、多功能信息显示标志物（B）复位后显示一张默认图片，选手需要通过执行翻页操作找到需要识别的有效车牌图片，有效车牌图片中仅包含 1 辆机动车（摩托车/货车/小轿车），其他类型图片为干扰图片；有效车牌图片中在不同位置存在 2 张及以上车牌，请依据图中车型识别对应的**有效车牌图片**（若图中车型为摩托车或货车，则有效车牌为黄底黑字车牌；若图中车型为小轿车，则有效车牌为渐变绿色车牌），其他颜色车牌为干扰车牌，数据无效。车牌显示格式为：“国 XYYYXY”。X 代表 A~Z 中任意一个字母（I 和 O 除外），Y 代表 0~9 中任意一个数字。
12	任务十一：竞赛平台（A）开启道闸任务 竞赛平台（A）由 B4 至 B2 的行进过程中，发送指定车牌信息开启道闸系统，在道闸栏杆落下前顺利通过道闸系统。	1、在练习赛道发送任意车牌均可开启道闸标志物，在测评赛道只有发送指定任务中识别的车牌(信息代码 M07)才能开启，开启一段时间之后（抬杆保持时间约为 7 秒），道闸标志物将自动关闭。

	之后竞赛平台（A）继续在 B4 至 B2 路段上行驶，到达 B2 处，自行选择位置避让竞赛平台（B）。	
13	任务十二：竞赛平台（A）完成立体显示控制 竞赛平台（A）位于 B2 位置，向位于 C3 处智能立体显示标志物发送数据，控制智能立体显示标志物显示文本信息。	1、智能立体显示标志物应在自定义文本累加显示模式下显示任务四获取的信息代码 M03。
14	任务十三：竞赛平台（B）交通灯识别任务 启动竞赛平台（B）行驶至在 B6 位置处，启动智能交通灯标志物(B) 进入识别模式，并在规定的时间内识别出当前停留信号灯的颜色，按照指定格式将正确信息发给智能交通灯标志物(B)进行确认。	1、竞赛平台（B）应在规定的时间内识别出交通灯信号颜色，并将识别结果按照指定格式发送至智能交通灯标志物，超时结果无效。 2、竞赛平台（B）识别后只需将结果返回至智能交通灯标志物(B)即可，无需执行其他操作。 3、竞赛平台（B）路径：B7→B6→B4→D4→D2→F2→车库
15	任务十四：竞赛平台（B）通过特殊地形任务 竞赛平台（B）由 B4 至 D4 行进路径中存在特殊地形标志物，竞赛平台（B）行进过程中禁止与特殊地形标志物两侧掩体发生碰撞。	1、特殊地形标志物放置位置为 C4 坐标点。 2、特殊地形标志物共计 6 张特殊地形卡片，可任意更换。测评赛道中所有参赛队地形卡片保持一致。
16	任务十五：竞赛平台（B）二维码识别 竞赛平台（B）从 D4 位置扫描 E4 处静态标志物（直）的二维码，并识别提取二维码中的有效信息按照指定格式发送到多功能信息显示标志物（B）(HEX 显示模式）显示。	1、静态标志物(A）内有一个二维码，二维码内包含数字“0-9”，大写字母”A-F”和特殊字符“{} +=”。有效信息仅包含大写字母和数字，格式固定为“XYXYXY”(其中 X 为大写字母，Y 为数字) 例：二维码数据为：{B1+D2E3=}，则有效信息为：B1D2E3。
17	任务十六：竞赛平台（B）语音交互任务 竞赛平台（B）由 D4 行进至 D2 位置处，进入语音识别模式，控制智能公交站标志物播报随机指令信息，竞赛平台（B）识别出播报的随机指令信息并进行重复播报	1、B 车在到达 D2 后，应发送随机播报语音指令控制智能公交站标志物发出语音信息，B 车识别语音信息后重复播报此条语音信息。 2、语音播报内容有：富强路站、民主路站、文明路站、和谐路站、爱国路站、敬业路站、友善路站。
18	任务十七：竞赛平台（B）停车入库任务（先入库） 竞赛平台（B）由 D2 行进至 F2 位置处,采用倒车方式驶入指定坐标的车库，立体车库 A 只能入库一辆车，竞赛平台（A）和竞赛平台（B）都有可能进入，但不会出现冲突的情况。	1、竞赛平台（B）应采用倒车入库的方式驶入指定车库。 2、立体车库有且仅有一个，可进行挡位控制，其余车库为虚拟车库入库点。 3、竞赛平台（B）最终入库的车库位置：信息代码 M04 的路灯的初始档位值对 2 取余加 1 得到的数据为车库位置，计算公式为：M04 % 2 + 1。计算结果是“1”时，则选择进入立体车库 A，如果是“2”时，则选择进入车库 B。 4、立体车库层数为竞赛平台（A）从任务八 RFID 卡内信息中提取的数据（M06）对 4 取余加 1 得到的数据为车库最终层数，计算公式为：M06 % 4 + 1。
19	任务十八：竞赛平台（A）顺利通过 ETC 系统任务 竞赛平台（A）到达 B2 处，使其智能 ETC 系统标志物开启然后顺利通过。	1、竞赛平台（A）需在不接触 ETC 栏杆（栏杆时间保持时间约为 10 秒）的情况下通过 ETC 系统。 2、选手应计算好通过时间，避免栏杆下落触碰竞赛平台（A）。若因此导致竞赛平台（A）失控，则视为选手控制不当，后果由选手自行承担。
20	任务十九：竞赛平台（A）停车入库任务（后入库） 竞赛平台（A）采用倒车方式驶入指定坐标的车库。立体车库 A 只能入库一辆车，竞赛平台（A）和竞赛平台（B）都有可能进入，但不会出现入库 A 冲突的情况。倒车入库后关闭智能显示标志物计时器模式,并开启无线充电标志物。	1、竞赛平台（A）应采用倒车入库的方式驶入指定车库。 2、立体车库有且仅有一个，可进行挡位控制，其余车库为虚拟车库入库点。 3、竞赛平台（A）最终入库的车库位置：信息代码 M04 的路灯的初始档位值对 2 取余得到的数据为车库位置，计算公式为：M04 % 2。计算结果是“0”时，则选择进入立体车库 C，如果是“1”时，则选择进入车库 A。

		4、立体车库层数为竞赛平台（A）从任务八 RFID 卡内信息中提取的数据（M06）对 4 取余加 1 得到的数据为车库最终层数，计算公式为：M06 % 4 + 1。

标志物摆放图


智能显示
智能公交站
智能立体车库（A）
竞赛平台（A）出发点
车库2
智能ETC系统
智能道闸
立体显示
静态显示（斜）
静态显示（直）
多功能信息显示（B）
特殊地形
智能交通信号灯（B）
智能交通信号灯（A）
智能报警台
竞赛平台（B）出发点
智能无线充电
智能路灯
多功能信息显示（A）
1
2
3
4
5
6
7
A
B
C
D
E
F
G

附件 1

数据处理算法

一、 DES 算法概述

DES（Data Encryption Standard）是一种对称加密算法，由 IBM 研制并在 1977 年被美国国家标准局（NIST）采纳为联邦信息处理标准（FIPS）。DES 算法使用相同的密钥对数据进行加密和解密，并且密钥的长度为 56 位。

DES 算法的基本原理是将明文数据分成一系列 64 位的数据块，然后通过一系列的加密操作将其转换为密文数据。加密过程中使用了一套复杂的置换、替代和混淆运算，包括初始置换(IP)、Feistel 网络、轮函数以及最终置换(IP-1)。

在加密过程中，DES 算法使用了一个 56 位长度的密钥，但实际有效密钥只有 48 位，因为每个密钥的第 8、16、24、32、40、48、56 位是奇偶校验位，用于校验密钥的正确性。DES 算法进行加密时，通过对密钥进行变换和混淆，产生 16 个子密钥，用于进行 16 轮的加密操作。

每一轮加密操作中，明文数据会被分成左右两个 32 位的数据块。然后，通过轮函数将右边的数据块与当前轮的子密钥进行处理，生成一个新的 32 位数据块。接着，将右边的数据块与左边的数据块进行异或运算，得到下一轮加密操作的输入数据。这样，经过 16 轮的运算，最后得到的左右两个数据块合并在一起，就是加密后的数据。

解密过程与加密过程相反，使用相同的密钥和运算过程，但是子密钥的应用顺序与加密时相反。

二、 基本原理

DES 算法通过一系列的置换、替代和混淆运算来加密和解密数据。下面详细介绍 DES 算法的原理：

说明：下图中⊕表示异或。

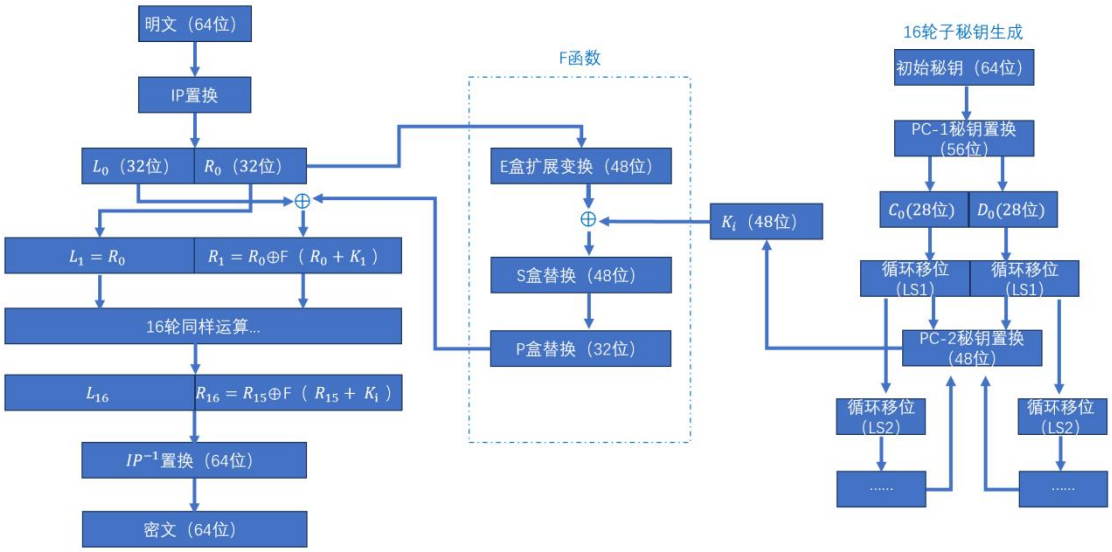


图 1 DES 算法加密流程图

1. IP 置换

置换可以简单地理解成【将明文打乱】——将原来的 64 位二进制位重新排序。其功能是把输入的 64 位数据块按位重新组合，并把输出分为 L_0、R_0两部分，每部分各长 32 位，其置换规则为将输入的第 58 位换到第一位，第 50 位换到第 2 位……依此类推，最后一位是原来的第 7 位。L0、R0 则是换位输出后的两部分，L0 是输出的左 32 位，R0 是右 32 位，例：设置换前的输入值为 D1D2D3……D64，则经过初始置换后的结果为：L0=D58D50……D8；R0=D57D49……D7。

表 1 IP 置换表

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

例如输入明文为：m=computer，用 ASCII 码表示为：

m = 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010

将明文进行 IP 置换，得：

IP = 11111111 10111000 01110110 01010111 00000000 11111111 00000110 100000011

2.秘钥初始化（PC-1 置换）

不考虑每个字节的第 8 位，DES 的密钥由 64 位减至 56 位，每个字节的第 8 位作为奇偶校验位。产生的 56 位密钥由下表生成（注意表中没有 8,16,24，32,40,48,56 和 64 这 8 位）：

表 2 PC-1 置换

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

由于上表中第一个元素为 57，这将使原秘钥的第 57 位变换为新秘钥 K+的第 1 位。同理，原秘钥的第 49 位变换为新秘钥的第 2 位，原秘钥的第 4 位变换为新秘钥的最后一位，注意原秘钥中只有 56 位会进入新秘钥，上表也只有 56 个元素，生成的新秘钥拆分为左右两个部分，C_0和 D_0，每半边都有 28 位。

例如输入的秘钥 K = 133457799BBCDFF1，用 ASCII 码表示为：

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

然后，将这个密钥拆分为左右两个部分，C0 和 D0，每半边都有 28 位：

C0 = 1111000 0110011 0010101 0101111

D0 = 0101010 1011001 1001111 0001111

3.16 轮秘钥迭代

秘钥需要进行 16 轮的迭代运算，每一个迭代运算生成一个子密钥，16 轮迭代运算（经过 16 轮相同运算）。通过下面流程图可知对于相同定义的 C0 和 D0，可创建 16 个块 Cn 和 Dn 1<=n<=16。

每一对 Cn 和 Dn 都是由前一对 Cn-1 和 Dn-1 移位而来。具体来说，对于 n=1,2,3，…，16，在前一轮移位的结果上，进行左移操作。什么叫左移？左移指的是将除第一位外的所有为往左移一位，将第一位移动至最后一位。

这意味着，比如说，C3 和 D3 是 C2 和 D2 移位而来的，具体来说，通过 2 次左移位，C16 和 D16 则是由 C15 和 D15 通过 1 次左移得到的。在所有情况下，一次左移就是将所有比特往左移动一位。使的一位后的比特的位置相较于变换前成为 2,3,4，…，28,1。

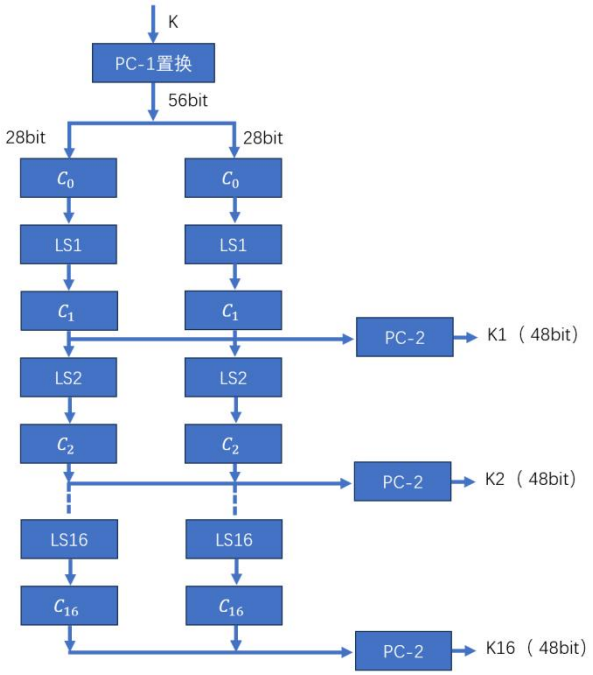


图 2 16 轮子秘钥迭代

现在可以得到第 n 轮的新秘钥 Kn（1<=n<=16）了。具体做法是，对每一对拼合后的子秘钥 CnDn，按照表 PC-2 执行变换，每对子秘钥有 56 位，但是 PC-2 仅仅使用其中 48 位。于是，第 n 轮新秘钥 Kn 的第一位来自组合秘钥 CnDn 的第 14 位，第 2 位来自第 17 位，以此类推，知道新秘钥的第 48 位来自组合秘钥的第 32 位。

表 2 PC-2 置换

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

4.F 函数运算

（1）E 盒扩展变换

输入的 64 位明文数据块经过 IP 置换后得到 L_0、R_0两部分，其中右半部分 R_0从 32 位扩展到 48 位(分为 4 位×8 组)输出，将 48 位结果与第 n 轮第密钥 K_n进行 XOR(异或)操作，将异或操作结果送入 S 盒进行压缩，压缩成 32 位,再将 32 位的结果送入 P 盒置换。

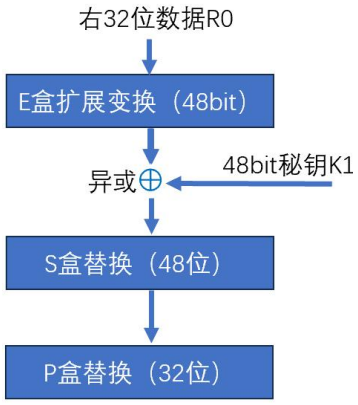


图 3 F 函数运算流程图

表 3 E 盒扩展变换

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

中间白色框部分表示置换后的明文两部分中的右半部分的位置信息，两列黄色数据是扩展的数据。例：第 1 位边上的 32 就是将第 32 位上的值复制一份到第 1 位的边上。也就是说 E(Rn-1)开头的三个比特分别来自 Rn-1 的第 32、1 和 2 位。E(Rn-1)末尾的 2 个比特分别来自 Rn-1 的第 32 位和第 1 位。

对输出 E（Rn-1）和秘钥 Kn 执行 XOR 运算：Kn⊕E(Rn-1)，其中⊕表示异或。

（2）压缩置换（S 盒代替）

将异或以后得到 48 位的数据送入 S 盒，进行替代运算。替代由 8 个不同的 S 盒完成，每个 S 盒有 6 位输入 4 位输出。48 位输入分为 8 个 6 位的分组，一个分组对应一个 S 盒，对应的 S 盒对各组进行代替操作，最后得到 32 位的数据。

表 4 S 盒 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

表 5 S 盒 2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

表 6 S 盒 3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

表 7 S 盒 4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	19
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

表 8 S 盒 5

2	12	4	1	7	10	11	6	5	8	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	13	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

表 9 S 盒 6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

表 10 S 盒 7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

表 11 S 盒 8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

一个 S 盒就是一个 4 行 16 列的表，盒中的每一项都是一个 4 位的数。S 盒的 6 个输入确定了其对应的输出在哪一行哪一列，输入的高低两位做为行数 H，中间四位做为列数 L，在 S-BOX 中查找第 H 行 L 列对应的数据(<32)。示例如下以 S1 盒为例：S 盒的 6 位输入为 101100，取最高位及最低位得到的值 10 转换为十进制为 2，除去最高位及最低位的四位数字组成 0110 转换为十进制为 6，则 S 盒的输出为行号为 2 列号为 6 所对应的值 2 的二进制 0010。

行号 \ 列号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

（3）P 盒置换

S 盒代替运算的 32 位输出按照 P 盒进行置换。该置换把输入的每位映射到输出位，任何一位不能被映射两次，也不能被略去，映射规则如下表：

表 12 P 盒置换

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

表中的数字代表原数据中此位置的数据在新数据中的位置，即原数据块的第 16 位放到新数据的第 1 位，第 7 位放到第 2 位，……依此类推，第 25 位放到第 32 位。

最后，P 盒置换的结果与最初的 64 位分组左半部分 L_0异或，然后左、右半部分交换，接着执行 16 个迭代，对 1<=n<=16,使用一个函数 F。函数 F 输入两个区块，一个 32 位的数据块和一个 48 位的秘钥区块 Kn，输出一个 32 位的区块。定义⊕表示异或。那么让 n 从 1 循环到 16，我们计算：

Ln=Rn-1

Rn=Ln-1+F(Rn-1,Kn)

5.IP-1 末置换

末置换是初始置换的逆过程，DES 最后一轮后，左、右两半部分并未进行交换，而是两部分合并形成一个分组做为末置换的输入。末置换规则如下表：

表 13 IP-1 末置换

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

也就是说，该变换的输出的第一位是输入的第 40 位，第二位是输入的 8 位，一直到将输入的第 25 位作为输出的最后一位，最后输出得到密文。

例如使用上述方法得到了第 16 轮的左右两个区块：

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100

R_{16} = 0000 1010 0100 1100 1101 1001 1001 0101

将两个区块调换位置，然后执行最终变换：

$R_{16}L_{16}$ = 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

IP-1 = 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101

解密就是加密的反过程，执行上述步骤，只不过在那 16 轮迭代中，调转左右子秘钥的位置而已。

三、 算法应用示例

如数据“0BCA8B4BEED9F7E0DF85F1A450BCE9A8”是在二维码（1）中“< >”内数据提取并经过加密后的十六进制数据，此数据作为 DES 算法的解密的数据并且均为有效数据。秘钥从二维码中（二维码（2））获取，如数据为“31<makelife>”，数据中只有< >里面的数据为有效数据，其余字符、标点符号等均为干扰数据，从而得知有效数据为“makelife”并把数据作为 DES 算法解密的秘钥，经过解密得出的原始数据为“1Skills2”，提取里面的英文字母则为“Skills”，通过转换为 ASCII 码后得出烽火台开启码为:0x53,0x6B,0x69,0x6C,0x6C,0x73