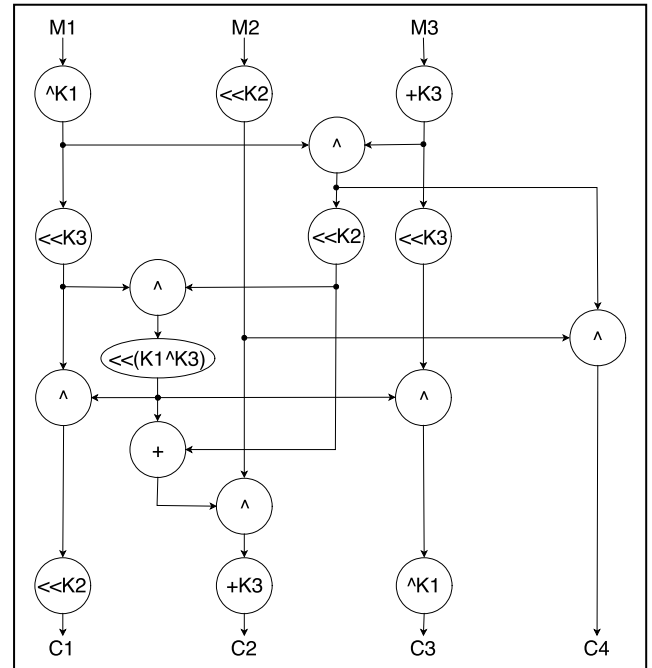




## Задача Н. Хакер

Налага се да проверите сигурността на вашата държава, като опитате да разбиете схемата за кодиране на националната агенция за сигурност. Имате няколко ключа и кодирани съобщения, но задачата изглежда невъзможна, тъй като нямате алгоритъма за декриптиране. По една щастлива случайност, късно през нощта, намирате на бюрото на шефа си диаграма на кодиращата схема (показана на фигурата) и откривате, че тя е лесна за разбиване. Напишете съответна програма за дешифриране.

Всяко 72-битово съобщение  $M$ , разделено на три 24-битови групи, означени отляво на дясно с  $M1$ ,  $M2$  и  $M3$ , се кодира в 96-битова шифрограма  $C$ , разделена на четири 24-битови групи – означени отляво на дясно с  $C1$ ,  $C2$ ,  $C3$  и  $C4$ , използвайки 72-битов ключ  $K$ , разделен на три 24-битови групи –  $K1$ ,  $K2$  и  $K3$ . Кодирането използва три операции над 24-битови операнди:



- **изключващо-или**, обозначено със знака  $\wedge$ ;
- **събиране по модул  $2^{24}$**  (стандартно събиране, игнориращо преноса към 25-тия бит, с който и без това не разполагаме), обозначено със знака  $+$ ;
- **циклично побитово изместване на ляво**, обозначено с  $\ll K$ , където  $K$  е броят на изместените битове (резултатът от операцията  $110101010001010011101010 \ll 7$ , например, е  $100010100111010101101010$ ).

**Вход:** На първия ред на стандартния вход ще бъде зададен броят  $T$  на тестовете. На всеки от следващите  $T$  реда ще са зададени по едно кодирано съобщение и ключът, с който е било кодирано – два низа с 24 и 18 шестнадесетични цифри, съответно, разделени с един интервал.

**Изход:** За всеки тестов пример, програмата трябва да изведе на отделен ред на стандартния изход низ, съдържащ 9-те ASCII символа на дешифрираното съобщение. Дешифрираните ASCII кодове са винаги съставени от печатуеми знаци (ASCII кодове от  $0x21$  до  $0x7e$ ). Всеки ASCII знак съответства на 8-те старши, средни или младши бита на всяка от групите  $M1$ ,  $M2$  и  $M3$  в този ред, като най-левият ASCII символ съответства на старшите 8 бита, вторият – на средните 8 бита, а третият – на младшите 8 бита на групата.

### Пример

Вход	Изход
2	BEAUTIFUL
971871216a9347c0eec722f9 953738ecc01feea4de	IMPORTANT
f3e3efdf6b318e15d36f7876 c37c26932a670b14d3	



## Task H. Hacker

You have to check the security of your state, trying to break the cryptosystem of the National security agency. You dispose of set of keys and corresponding crypto texts, but the task seems unsolvable, because you don't know the decrypting algorithm. Accidentally, late in the night, you find on the desk of the chief a diagram of the crypto scheme (shown on the figure) and realize that it is easy for breaking. Write the corresponding decrypting program.

Each 72-bit message  $M$ , split in three 24-bit groups, denoted from left to right by  $M1$ ,  $M2$  and  $M3$ , is coded to 96-bit crypto text  $C$ , split in four 24-bit groups, denoted from left to right by  $C1$ ,  $C2$ ,  $C3$  and  $C4$ , using 72-bit key  $K$ , split in three 24-bit groups –  $K1$ ,  $K2$  и  $K3$ . Coding uses three operations over 24-bit operands:

- *exclusive-or*, denoted by  $\wedge$ ;
- *addition modulo  $2^{24}$*  (usual addition, with ignoring of 25-th bit, if any), denoted by  $+$ ;
- *cyclic bitwise shift left*, denoted by  $\ll K$ , where  $K$  is the number of shifted bits (for example, the result of  $110101010001010011101010 \ll 7$  is  $100010100111010101101010$ ).

**Input:** On the first line of the standard input the number  $T$  of the tests will be given. Each of the next  $T$  lines will contain one crypto message and the key used for coding it – two hexadecimal strings with 24 and 18 digits, respectively, separated by one interval.

**Output:** For each test case the program has to print on a separate line of the standard output the 9 ASCII characters of the decrypted message. Decrypted ASCII codes will be always printable characters (ASCII codes from  $0x21$  to  $0x7e$ ). Each ASCII character correspond to 8 left, middle or right bits of each of the groups  $M1$ ,  $M2$  and  $M3$  in such order – the first ASCII character corresponds to the leftmost 8 bits, second – to the middle 8 bits, and the third – to the rightmost 8 bits of the group.

### Example

Input	Output
2	BEAUTIFUL
971871216a9347c0eec722f9 953738ecc01feea4de f3e3efdf6b318e15d36f7876 c37c26932a670b14d3	IMPORTANT

