ä½ å¥½ï¼Œæˆ‘æ˜¯æœ±ç»´å¨šã€‚æ¬¢è¿Žä½ ç»§ç»è·Ÿæˆ‘å¦ä¹ ç¿»æ€§ä»£æ•°ã€‚

ä»Šå¤©æˆ‘è¦è®²çš„å†…å®¹æ˜¯â€œå¦‚ä½•é€šè¿‡æœ‰é™å‘é‡ç©ºé—´åŠ æ¢çš„å¸Œå°”ä¼¯ç‰¹ç©ºé—´å‘æŠ€ä¸ºä¸€ä¸ªé€€åŒ–çš„å›¾æ‹ŸåŒæ€ã€‚

è¿™ç¯‡çš„å†…å®¹ï¼šéžå¸¸æœ‰è¶£ï¼Œæˆ‘å’Œå¤§å®¶åˆ†äº«ä¸€ä¸ªæ•…äº‹ï¼Œæ˜¯å…³äºŽäºŒæˆ˜æ—¶æœŸçš„ä¸€ä½è‹±å›½å¤©æ‰ï¼Œä»–æ˜¯äººå·¥æ™ºèƒ½ä¹‹çˆ¶ï¼Œä»–ç ´è¯‘äº†å¾·å›½çš„å¯†ç æœºï¼ˆEnigmaï¼‰ï¼Œå¸®åŠ©ç›Ÿå†›æ‰“èµ¢äº†æˆ˜äº‰ã€‚

ä¸è¿‡ç”µå½±æ¯•ç«Ÿæ˜¯ç”µå½±ï¼Œæœ‰è®¸å¤šå†…å®¹æ˜¯ä¸çŽ°å®žçš„ï¼Œå¥½åœ¨è¡¨è¾¾å‡ºæ¥çš„ç ´è¯‘æ©å°¼æ ¼çŽ›å¯†ç çš„æ ¸å¿ƒè§‚ç‚¹æ˜¯æ£ç¡®çš„ã€‚è¦ç ´è¯‘ä¸€ä»½è¢«æ©å°¼æ ¼çŽ›æœºåŠ å¯†çš„å¯†æ–‡ï¼Œéœ€è¦è¿™ä¸‰ç±»ä¿¡æ¯ï¼š

1. æ©å°¼æ ¼çŽ›æœºçš„åŸºæœ¬åŽŸç†åŠå†…éƒ¨æž„é€ ï¼ŒåŒ…æ‹¬æ¯ä¸ªè½¬åçš„ç»“æž„ï¼›
2. å¾·å†›å¯¹æ©å°¼æ ¼çŽ›æœºçš„æ“ä½œå®ˆå‰™ï¼›
3. å¾·å†›æ‰€ä½¿ç”¨çš„æ¯æ—¥åˆå§‹è®¾ç½®ã€‚æ©å°¼æ ¼çŽ›æœºçš„æ¯æ—¥åˆå§‹è®¾ç½®åŒ…æ‹¬ä¸‰ä¸ªè½¬åçš„æŽ’åˆ—é¡ºåºä»¥åŠæ¯ä¸ªè½¬åçš„åˆå§‹ä½ç½®ï¼Œä»¥åŠæ’çº¿æ¿çš„è®¾ç½®ã€‚è¿™äº›ä¿¡æ¯ä¼šåœ¨æ¯å¤©åˆå¤œæ›´æ¢ï¼Œå³æ¯24å°æ—¶æ›´æ¢ä¸€æ¬¡è®¾ç½®ï¼Œæ¯æœˆæ›´æ¢ä¸€æ¬¡å¯†ç æœ¬ã€‚

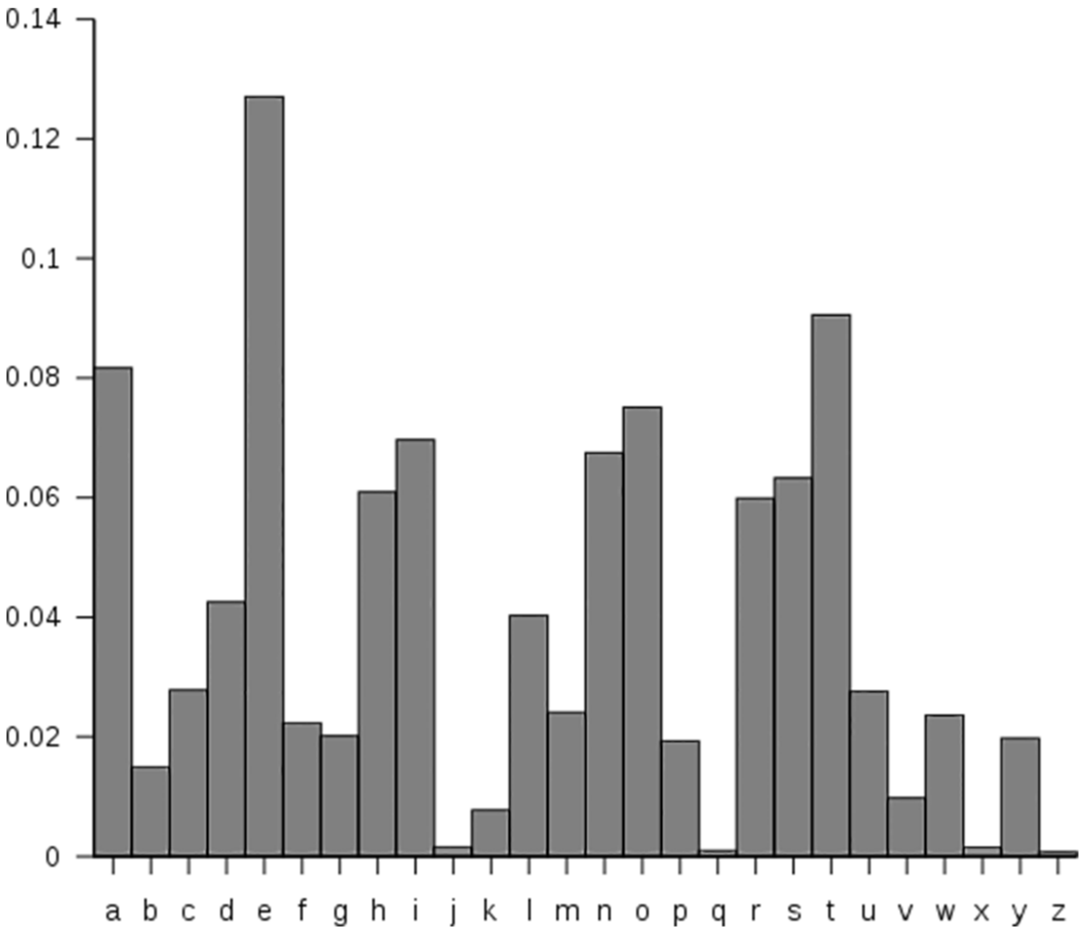
è¿™äº›åœ¨ç”µå½±é‡Œç®€åŒ–äº†ï¼Œä½†æˆ‘ä»¬è¦è®²ä¸‹é¢çš„é‡ç‚¹ï¼Œå°±æ˜¯æ©å°¼æ ¼çŽ›å¯†ç æœºçš„æœ¬èº«ã€‚

ä¸ºä»€ä¹ˆé€‰æ‹©å¸Œå°”ä¼¯ç‰¹ç©ºé—´ï¼Ÿ

è¦è®²å¯†ç ï¼Œæˆ‘ä»¬å¾—å…ˆçŸ¥é“ä»€ä¹ˆæ˜¯ä»€ä¹ˆå«é€‰æ‹©ã€‚

æœ€å¤è€çš„æœ€ç®€å•çš„å¯†ç å—æ³•ï¼Œæ˜¯å‡¯æ’’å¯†ç ï¼Œå®ƒçš„åŽŸç†æ˜¯å°†æ¯ä¸ªå—æ¯æ›¿æ¢ä¸ºå—æ¯è¡¨ä¸ç›¸éš”å›ºå®šä½ç½®çš„å¦ä¸€ä¸ªå—æ¯ã€‚

ä¸¾ä¸ªä¾‹åï¼Œå¦‚æžœæˆ‘ä»¬è¦åŠ å¯†ä¸€æ®µæ–‡å—ï¼Œå°±å°†æ¯ä¸ªå—æ¯å‘åŽç§»åŠ¨ä¸‰ä½ã€‚



ä¸Šé¢è¿™å¼ å›¾æ¥è‡ªç»´åŸºç™¾ç§'ï¼Œæ˜¾ç¤ºçš„æ˜¯26ä¸ªå—æ¯åœ¨æ™®é€šçš„è‹±æ–‡æ–‡æœ¬ä¸å‡ºçŽ°çš„æ¦‚çŽ‡ã€‚

åªè¦æˆ'ä»¬èƒ½å¤ŸèŽ·å–è¶³å¤Ÿé•¿çš„å¯†æ–‡è¿›è¡Œåˆ†æžçš„è¯ï¼Œé€šè¿‡å—æ¯å‡ºçŽ°çš„é¢'çŽ‡ï¼Œæˆ'ä»¬å°±èƒ½å¤ŸçŒœå‡ºç›¸åº"çš„åŽŸå§‹å—æ¯ï¼Œè¿™å¹¶ä¸å®‰å…¨ã€‚æ‰€ä»¥ï¼Œé€šç"¨æ€§é«˜æ€§èƒ½å¼ºçš„æ›¿æ¢å¯†ç ï¼Œä»Žè€Œæ›´å®¹æ˜"ç ´è§£ã€‚èƒ½å¤Ÿé˜²æ¢é¢'çŽ‡åˆ†æžæ"»å‡»çš„å¯†ç ï¼Œå…¶ä¸å¸Œå°"åŠ å¯†å°±æ˜¯ä¸€ä¸ªè¾ƒå¥½çš„é€‰æ‹©ï¼Ÿ

å¸Œå°"å¯†ç åŽŸç†

æˆ'ä»¬å…ˆæ¥çœ‹ä¸€ä¸‹å¸Œå°"å¯†ç çš„åŽŸç†ã€‚æ ¹æ®ç™¾åº¦ç™¾ç§'çš„å®šä¹‰ï¼Œå¸Œå°"å¯†ç ï¼ˆHill Cipherï¼‰æ˜¯è¿ç"¨åŸºæœ¬çŸ©é˜µè®ºåŽŸç†çš„æ›¿æ¢å¯†ç ï¼Œç"±Lester S. Hillåœ¨1929å¹´å'æ˜Žã€‚æ¯ä¸ªå—æ¯å½"ä½œ26è¿›åˆ¶æ•°å—ï¼šA=0ï¼ŒB=1ï¼ŒC=2â€¦ ï¼ŒæŠŠä¸€ä¸²å—æ¯å½"æˆnç»´å'é‡ï¼Œå'Œä¸€ä¸ª$nÃ—n$çš„çŸ©é˜µç›¸ä¹˜ï¼Œå†å°†å¾—å‡ºçš„ç»"æžœå'Œ26è¿›è¡Œæ¨¡è¿ç®—ã€‚

æ‰€ä»¥ï¼Œå¸Œå°"åŠ å¯†ç®—æ³•çš„åŸºæœ¬æ€æƒ³æ˜¯ï¼Œé€šè¿‡çº¿æ€§å˜æ¢å°†å¤šä¸ªæ˜Žæ–‡å—æ¯è½¬æ¢ä¸ºåŒæ ·æ•°é‡çš„å¯†æ–‡å—æ¯ï¼Œè§£å¯†åªè¦ä½œä¸€æ¬¡é€†å˜æ¢å°±å¯ä»¥äº†ï¼Œè€Œå¯†é'¥å°±æ˜¯å˜æ¢çŸ©é˜µæœ¬èº«ã€‚

çŽ°åœ¨ï¼Œæˆ'ä»¬å†é€šè¿‡æ•°å¦çš„æ–¹å¼æ¥è¡¨è¾¾ä¸€ä¸‹ï¼Œå¸Œå°"å¯†ç æ˜¯å¦‚ä½•é€šè¿‡ä¸‰æ¥æ¥å®žçŽ°åŠ å¯†çš„ã€‚

ç¬¬ä¸€æ¥ï¼Œè®¾ç½®åŠ å¯†çŸ©é˜µEã€‚

ç¬¬äºŒæ¥ï¼Œå¯¹ç…§å—æ¯ç¼–ç è¡¨ï¼ˆè‡ªè¡Œè®¾å®šï¼‰å¾—å°æ•°å—ï¼Œå¹¶æŠŠæ˜Žæ–‡æ¶ˆæ¯åˆ†å‰²æˆå¤§å°ä¸ºnçš„å¤šä¸ªå—ï¼š$v_{1},v_{2},â€¦$ï¼Œå¹¶ä¸"å¿ç•¥ç©ºæ ¼ã€‚è¿™é‡Œä¹‹æ‰€ä»¥å¿ç•¥ç©ºæ ¼ï¼Œæ˜¯å› ä¸ºè¦æf…
å†µä¸‹å¯†ç ä¼ é€'çš„ä¿¡æ¯ä¸è¶³ä»¥è¡¥é½ä¸ªæ•°ã€‚å¦‚æžœå¯†ç è¡¥é½ä¸ªæ•°ï¼Œæ˜¯å¯ä»¥å†å¤šæ¬¡ä¼ é€'çš„ã€‚è¿™é‡Œçš„nè¡¨ç¤ºçš„å¯†é'¥çš„é˜¶æ•°ï¼Œå¯†é'¥çš„é˜¶æ•°è¶Šé«˜ï¼Œä¹Ÿå°±æ˜¯nè¶Šå¤§çš„è¯ï¼Œç ´è¯'çš„éš¾åº¦ä¹Ÿå°±è¶Šå¤§ã€‚

ç¬¬ä¸‰æ¥ï¼Œæ¯ä¸ªæ¶ˆæ¯å—å'ŒåŠ å¯†çŸ©é˜µEç›¸ä¹˜ï¼š$Ev_{1}, Ev_{2},â€¦$ï¼Œå¹¶å'Œ26è¿›è¡Œæ¨¡è¿ç®—ï¼Œæœ€åŽå¯¹ç…§å—æ¯ç¼–ç è¡¨å¾—åˆ°å¯†æ–‡ã€‚

åŒæ ·ï¼Œæˆ'ä»¬æŠŠè¿™ä¸‰æ¥å€'è¿‡æ¥ï¼Œå°±èƒ½å®žçŽ°è§£å¯†äº†ã€‚

ç¬¬ä¸€æ¥ï¼Œè®¡ç®—åŠ å¯†çŸ©é˜µEçš„é€†çŸ©é˜µ$D \equiv E^{-1}(\bmod 26)$ã€‚

ç¬¬äºŒæ¥ï¼Œå¯¹ç…§å—æ¯ç¼–ç è¡¨å¾—åˆ°æ•°å—ï¼ŒæŠŠå®ƒå'Œè§£å¯†çŸ©é˜µDç›¸ä¹˜ï¼Œå¹¶å'Œ26è¿›è¡Œæ¨¡è¿ç®—ã€‚

ç¬¬ä¸‰æ¥ï¼Œå¯¹ç…§ç¼–ç è¡¨ï¼Œå¾—åˆ°åŽŸå§‹æ˜Žæ–‡ã€‚

è¿™é‡Œä½ éœ€è¦æ³¨æ„çš„æ˜¯ï¼ŒåŠ å¯†çŸ©é˜µå¾ˆå…³é"®ï¼Œå®ƒå°±æ˜¯æˆ'ä»¬é€šå¸¸æ‰€è¯´çš„â€œå¯†é'¥â€ï¼Œä¹Ÿå°±æ˜¯æ‰"å¼€å¯†ç çš„é'¥åŒ™ã€‚

é€šè¿‡å‰é¢è®²è§£çš„åŠ å¯†è§£å¯†æ¥éª¤ï¼Œæˆ'ä»¬å¯ä»¥çœ‹å‡ºï¼Œå¸Œå°"å¯†ç ä¹‹æ‰€ä»¥å¾ˆéš¾è¢«ç ´è¯'ï¼Œæ˜¯å› ä¸ºå®ƒè®¾ç½®äº†ä¸‰é"å…³å¡ï¼š

1. åˆ—çŸ©é˜µçš„ç»´åº¦æœªçŸ¥ï¼›
2. å¯¹åº"å—æ¯è¡¨çš„æŽ'åˆ—æœªçŸ¥ï¼›
3. åŠ å¯†çŸ©é˜µï¼ˆæˆ–è€…è¯´å¯†é'¥ï¼‰æœªçŸ¥ã€‚

æƒ³è¦ç ´è§£å¸Œå°"å¯†ç ï¼Œå°±éœ€è¦åŒæ—¶èŽ·å–åˆ°é€šè¿‡è¿™ä¸‰é"å…³çš„é'¥åŒ™ï¼Œè¿™è°ˆä½•å®¹æ˜"ã€‚

å¸Œå°"å¯†ç å®žä¾‹

å¥½äº†ï¼ŒåŽŸç†éƒ½è®²å®Œäº†ï¼ŒçŽ°åœ¨æˆ'ä»¬é€šè¿‡ä¸€ä¸ªä¾‹åæ¥å®žé™…åœ°çœ‹ä¸€ä¸‹å¸Œå°"å¯†ç åŠ å¯†å'Œè§£å¯†çš„è¿‡ç¨‹ã€‚

å‡è®¾ï¼šAå'ŒBåŒæ–¹æœ‰ä¸€æ¡é‡è¦æ¶ˆæ¯è¦ä¼ é€'ï¼ŒåŒæ–¹å¾ˆæ—©å°±å»ºç«‹äº†å¯†é'¥ä¼ é€'æœºåˆ¶ï¼Œæ¯è¿‡ä¸€æ®µæ—¶é—´éƒ½ä¼šæ›´æ–°å¯†é'¥ã€‚åœ¨è¿™æ¬¡çš„å¯†é'¥æ›´æ–°åˆ°æœŸä¹‹ï¼Œæ£ç¡®çš„å¯†é'¥ï¼Œä¹Ÿå°±æ˜¯åŠ å¯†çŸ©é˜µæ˜¯ä¸€ä¸ª3Ã—3çŸ©é˜µã€‚

$$
E=\left[\begin{array} {ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15

\end{array}\right]
$$

è¿™ä¸€æ¬¡Aè¦ç»™Bçš„æ¶ˆæ¯æ˜¯â€œILIKEBODYCOMBATâ€ï¼Œæˆ'ä»¬ç"¨ä¹‹å‰çš„ä¸‰é˜¶åœ¨Aæ–¹å…ˆæ¥åŠ å¯†ï¼š

ç¬¬ä¸€æ¥ï¼Œå®šä¹‰åŠ å¯†çŸ©é˜µï¼Œä¹Ÿå°±æ˜¯åˆšæ‰çš„EçŸ©é˜µã€‚

字母编码表

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
N	O	P	Q	R	S	T	U	V	W
13	14	15	16	17	18	19	20	21	22

ç¬¬äºŒæ¥ï¼Œå¯¹ç…§å—æ¯ç¼–ç è¡¨å°†æ•°å—ï¼š8ã€11ã€8ã€10ã€4ã€1ã€14ã€3ã€24ã€2ã€14ã€12ã€1ã€0ã€19ã€‚æŽ¥ä¸‹æ¥ï¼ŒæŠŠæ˜Žæ–‡æ¶ˆæ¯åˆ†å‰²æˆå¤§å°ä¸º3çš„5ä¸ªå—ï¼Œä¹Ÿå°±æ˜¯ç»´åº¦ä¸º3çš„5ä¸ªåˆ—
çŸ©é˜µã€‚

$$
v_{1}=\left[\begin{array}{c}
8 \\\
11 \\\
8
\end{array}\right], v_{2}=\left[\begin{array}{c}
10 \\\
4 \\\
1
\end{array}\right], v_{3}=\left[\begin{array}{c}
14 \\\
3 \\\
24
\end{array}\right], v_{4}=\left[\begin{array}{c}
2 \\\
14 \\\
12
\end{array}\right], v_{5}=\left[\begin{array}{c}
1 \\\
0 \\\
19
\end{array}\right]
$$

ç¬¬ä¸‰æ¥ï¼Œå°†æ¯ä¸ªæ¶ˆæ¯å—å'ŒåŠ å¯†çŸ©é˜µEç›¸ä¹˜ï¼š

$$
E v_{1}=\left[\begin{array}{ccc}
6 & 24 & 1 \\\
13 & 16 & 10 \\\
20 & 17 & 15
\end{array}\right]\left[\begin{array}{c}
8 \\\
11 \\\
8
\end{array}\right]=\left[\begin{array}{c}
320 \\\
360 \\\
467
\end{array}\right] \bmod 26=\left[\begin{array}{c}
8 \\\

22 \\
25
\end{array}\right]
$$

$$
E v_{2}=\left[\begin{array}{ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15
\end{array}\right]\left[\begin{array}{c}
10 \\
4 \\
1
\end{array}\right]=\left[\begin{array}{c}
157 \\
204 \\
283
\end{array}\right] \bmod 26=\left[\begin{array}{c}
1 \\
22 \\
23
\end{array}\right]
$$

$$
E v_{3}=\left[\begin{array}{ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15
\end{array}\right]\left[\begin{array}{c}
14 \\
3 \\
24
\end{array}\right]=\left[\begin{array}{c}
180 \\
470 \\
691
\end{array}\right] \bmod 26=\left[\begin{array}{c}
24 \\
2 \\
15
\end{array}\right]
$$

$$
E v_{4}=\left[\begin{array}{ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15
\end{array}\right]\left[\begin{array}{c}
2 \\
14 \\
12
\end{array}\right]=\left[\begin{array}{c}
360 \\
370 \\
458
\end{array}\right] \bmod 26=\left[\begin{array}{c}
22 \\
6 \\
16
\end{array}\right]
$$

$$
E v_{5}=\left[\begin{array}{ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15
\end{array}\right]\left[\begin{array}{c}
1 \\
0 \\
19
\end{array}\right]=\left[\begin{array}{c}
25 \\
203 \\
305
\end{array}\right] \bmod 26=\left[\begin{array}{c}
25 \\
21 \\
19
\end{array}\right]
$$

æœ€åŽï¼Œå¯¹ç…§å—æ¯ç¼–ç è¡¨å¾—åˆ°å¯†æ–‡ï¼šâ€œIWZBWXBCGWGQZVTâ€ã€‚

Bæ‹¿åˆ°è¿™ä¸ªå¯†æ–‡åŽï¼Œä½¿ç”¨ä¸‹æ¥æ¥è§£å¯†ï¼š

ç¬¬ä¸€æ¥ï¼Œè®¡ç®—åŠ å¯†çŸ©é˜µEçš„é€†çŸ©é˜µDï¼š

$$
D \equiv\left[\begin{array}{ccc}
6 & 24 & 1 \\
13 & 16 & 10 \\
20 & 17 & 15
\end{array}\right]^{-1}(\bmod 26) \equiv\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]
$$

ç¬¬äºŒæ¥ï¼Œå¯¹ç…§å—æ¯ç¼–ç è¡¨å¾—åˆ°æ•°å—ï¼ŒæŠŠå¯†æ–‡è§£å¯†çŸ©é˜µDç›¸ä¹˜ï¼Œå¹¶å¯¹26è¿›è¡Œæ¨¡è¿ç®—ï¼Œå¾—åˆ°çš„ç»“æžœã€‚

$$

\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]\left[\begin{array}{c}
8 \\
22 \\
25
\end{array}\right]=\left[\begin{array}{c}
424 \\
869 \\
632
\end{array}\right] \bmod 26=\left[\begin{array}{c}
8 \\
11 \\
8
\end{array}\right]
$$

$$
\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]\left[\begin{array}{c}
1 \\
22 \\
23
\end{array}\right]=\left[\begin{array}{c}
348 \\
680 \\
469
\end{array}\right] \bmod 26=\left[\begin{array}{c}
10 \\
4 \\
1
\end{array}\right]
$$

$$
\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]\left[\begin{array}{c}
24 \\
2 \\
15
\end{array}\right]=\left[\begin{array}{c}
352 \\
835 \\
648
\end{array}\right] \bmod 26=\left[\begin{array}{c}
14 \\
3 \\
24
\end{array}\right]
$$

$$
\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]\left[\begin{array}{c}
22 \\
6 \\
16
\end{array}\right]=\left[\begin{array}{c}
366 \\
846 \\
662
\end{array}\right] \bmod 26=\left[\begin{array}{c}
2 \\
14 \\
12
\end{array}\right]
$$

$$
\left[\begin{array}{ccc}
8 & 5 & 10 \\
21 & 8 & 21 \\
21 & 12 & 8
\end{array}\right]\left[\begin{array}{c}
25 \\
21 \\
19
\end{array}\right]=\left[\begin{array}{c}
495 \\
1092 \\
929
\end{array}\right] \bmod 26=\left[\begin{array}{c}
1 \\
0 \\
19
\end{array}\right]
$$

æœ€åŽï¼ŒBé€šè¿‡å¯¹ç…§ç¼–ç è¡¨ï¼Œå¾—åˆ°äº†åŽŸå§‹æ˜Žæ–‡ï¼šâ€œILIKEBODYCOMBATâ€ã€‚

è¿™é‡Œï¼Œä½ ä¹Ÿè®¸ä¼šé—®ï¼Œå¯†é’¥ä¸ºä»€ä¹ˆç”¨çš„æ˜¯3Ã—3çš„å¯é€†çŸ©é˜µï¼Ÿé‚£æ˜¯æˆ‘ä¸ºäº†ä¸¾ä¾‹æ–¹ä¾¿è€Œè®¾ç½®çš„ï¼Œä½ å®Œå…¨å¯ä»¥è®¾ç½®æ›´é«˜é˜¶çš„çŸ©é˜µã€‚å°±åƒä¹‹å‰è´çš„ï¼Œå¯†é’¥çš„é˜¶æ•°è¶Šé«˜ï¼Œä¹Ÿå°±æ˜¯nè¶Šå¤§çš„è¯ï¼Œç ´è§£çš„éš¾åº¦ä¹Ÿå°±è¶Šå¤§ï¼Œæ‰€éœ€è¦çš„è®¡ç®—é‡ä¹Ÿå°±è¶Šå¤§ã€‚

æ‰€ä»¥ï¼Œä»Žç ´è§£çš„è§'åº¦æ¥çœ‹ï¼Œä¼ ç»Ÿçš„å¯†ç æœ‰ä¸€ä¸ªè‡´å'½å¼±ç‚¹ï¼Œå°±æ˜¯ç ´è§£è€…可以ä»Žç»Ÿè®¡å¦è§'åº¦æ¥ç ´è§£å—ç¬¦é¢'çŽ‡ä¸Žæ‰¾åˆ°è§„å¾‹ï¼Œè¿›è€Œæ‰¾å‡ºç ´è§£çš„çªç ´å£ã€‚å°¤å…¶æ˜¯åœ¨è®¡ç®—æœºæŠ€æœ¯é«˜åº¦å'è¾¾çš„ä»Šå¤©ï¼Œç ´è§£çš„é€Ÿåº¦æ›´å¿«äº†ã€‚è€Œå¸Œå°”å¯†ç ç®—æ³•å®Œå…¨å…‹æœäº†è¿™ä¸€ç¼ºé™·ï¼Œå®ƒé€šè¿‡é‡‡ç"¨çŸ©é˜µè¿ç®—çš„æ–¹æ³•æ¥ä»ç©ºåŸºç¡€ï¼Œç¨³å®šäº†çŸ©é˜µæ•°æ—¹ç®——

å’Œé€†è¿ç®—ï¼Œè ƒ½å¤Ÿè¾ƒå¥½åœ°æŠµæŠ—é¢‘çŽ‡å ˆ†æžï¼Œå¾ˆéš¾è¢«æ”»ç ´ã€‚

æœ¬èŠ‚å°ç»“

è¿™ä¸€èŠ‚è¯¾çš„å†…å®¹éƒ½å’Œå¯†ç å¦æœ‰å…³ï¼Œæ„Ÿè§‰å ƒæ˜¯æŒºæœ‰æ„æ€çš„ã€‚ä½†å…¶å®žå®žåœ¨çš„æ ¸å¿ƒç®—æ³•ï¼Œå°±æ˜¯é€šè¿‡åŸºç¡€ç‰ä¸å¦å‰çš„çŸ©é˜µå’Œé€†çŸ©é˜µçš„çŸ¥è¯†ï¼Œæ¥å®žçŽ°åŠ å¯†å’Œè§£å¯ ã€‚åŠ å¯ çš„å…³é”®å°±æ˜¯å®šä¹‰åŠ å¯†çŸ©é˜µï¼Œæˆ–è€…è¯´å¯†é’¥ã€‚å—æ¨¡æ‹Ÿçš„ï¼Œçœ‹çœ‹ã€‚å…ˆçŸ©é˜µçš„ç›´ä¹‰ï¼Œé€šè¿‡çº¿æ€§å˜æ¢å°†å›°å®šæ•°é‡çš„æ˜Žæ–‡å—æ˜ å°„åˆ°æ•°é‡çš„å¯†æ–‡å—ï¼Œè€Œè§£å¯ †å™¨è¦ä½œä¸€æ¬¡é€†å˜æ¢å°±å¯ä»¥äº†ã€‚

å½“ç„¶ï¼ŒçŽ°å®žä¸è¿˜æœ‰æ›´å¤æ‚çš„åŠ å¯†ç®—æ³•ï¼Œå…¶ä¸æœ€è‘—åçš„ï¼Œä¹Ÿç”¨åˆ°çº¿æ€§ä»£æ•°çš„åŠ å¯†ç®—æ³•æ˜¯AESï¼Œæƒ³å¿…ä½ å¹³æ—¶ä¹Ÿç»å¸¸å¬åˆ°è¿™ä¸ªè¯ã€‚AESæ˜¯ä¸€ä¸ªè¿ä»£çš„ã€å¯¹ç§°å¯†é’¥åˆ†ç»„çš„å¯†ç ï¼Œå®ƒå¯ä»¥ä½¿ç”¨128ã€192å’Œ256ä½å¯†é’¥ï¼Œå¹¶ä¸”ç”¨128ã€192å’Œ256ä½åˆ†ç»„åŠ å¯†å’Œè§£å¯†æ•°æ®ï¼Œå…¶ä¸å¯†é’¥é•¿åº¦ä¸Žåˆ†ç»„é•¿åº¦æ˜¯ç‹¬ç«‹çš„ã€‚

çº¿æ€§ä»£æ•°ç»ƒä¹ åœº

è¯·ä½ å°±ä»¥å»ºä½œ“MACHINELEARNING”ä½œä¸ºæ˜Žæ–‡ï¼Œåº”è¯¥ç”¨ä¸åŒçš„çŸ©é˜µä¸ªåˆ†å«åŠ å¯†å’Œè§£å¯†ã€‚

> æç¤ºï¼šä½ å¯ä»¥è‡ªè¡Œå®šä¹‰åŠ å¯†çŸ©é˜µå€¼ï¼Œæ¯”å¦‚ç»™ä¸ªä»‹äºŽå¯é€†å¯¹ç§°çŸ©é˜µçš„ç»´åº¦ã€‚åŠ å¯†çŸ©é˜µå¯ä»¥ä½¿ç”¨ä¹‹å‰ä»‹ç»çš„3Ã—3å¯é€†çŸ©é˜µï¼Œä¹Ÿå¯ä»¥ä½¿ç”¨å…¶å®ƒnÃ—nçš„å¯é€†çŸ©é˜µã€‚

æ¬¢è¿Žåœ¨ç•™è¨€åŒºæ™’å‡ºä½ çš„åŠ å¯†å’Œè§£å¯†è¿‡ç¨‹ï¼Œæˆ‘ä¼šåŠæ—¶å›žå¤ã€‚åŒæ—¶ï¼Œä¹Ÿæ¬¢è¿Žä½ æŠŠè¿™ç¯‡æ–‡ç« åˆ†äº«ç»™ä½ çš„æœ‹å‹ï¼Œä¸€èµ·è®¨è®ºã€å¦ä¹ ã€‚