Part 1: Cryptography

- Cryptography describes how to transfer messages between participants without anyone else being able to read or modify them
- Prerequisite for Computer Security
- Start module with explaining the basics of cryptography (enough to understand how TLS works; for more details see cryptography module)
- Before we start with Cryptography, need to look at how to represent data

Codes versus Ciphers

Codes vs. Ciphers

- A code is any way to represent data.
 Will use bitstrings (sequence of bits) to represent data.
 Examples:
 - Morse Code, ASCII, Hex, Base64
- A cipher is a code where it is difficult to derive data from code.
 - Almost always uses a key.
 - Data for a cipher usually called plain text, encoding called cipher text
 - Function from plain text to cipher text called encryption
 - Function from cipher text to plain text called decryption

Codes vs. Ciphers

What is "27" encoded in binary?

- 0001 1011
- 0010 0111
- 110110 111011
- 0011 0010 0011 0111
- All of the above

Codes vs. Ciphers

What is "27" encoded in binary?

• 0001 1011 27 as decimal

• 0010 0111 27 as hex

• 110110 111011 27 as Base64

• 0011 0010 0011 0111 27 as ASCII

• All of the above Yes

Hex

- Characters 0 to F encode 4 bits
- Easiest way to write down binary as text

```
0 = 0000 8 = 1000

1 = 0001 9 = 1001

2 = 0010 A = 1010

3 = 0011 B = 1011

4 = 0100 C = 1100

5 = 0101 D = 1101

6 = 0110 E = 1110

7 = 0111 F = 1111
```

ASCII

0x02 2 STX Start of text 0x22 34 " 0x42 66 B 0x62 98 b 0x03 3 ETX End of text 0x23 35 # 0x43 67 C 0x63 99 b 0x04 4 EOT End of transmission 0x24 36 0x44 68 D 0x64 100 d 0x05 5 ENQ Enquiry 0x25 37 % 0x45 69 E 0x65 101 e 0x06 6 ACK Acknowledge 0x26 38 & 0x46 70 F 0x65 101 e 0x07 7 BELL Bell 0x27 39 0x47 71 G 0x67 103 g 0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x66 102 10 10 10 10 10 10 10 10 10 <th>Hex</th> <th></th> <th>Char</th> <th></th> <th>Hex</th> <th>Dec</th> <th>Char</th> <th>Hex</th> <th>Dec</th> <th>Char</th> <th>Hex</th> <th>Dec</th> <th>Char</th>	Hex		Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x02 2 STX Start of text 0x22 34 " 0x42 66 B 0x62 98 b 0x03 3 ETX End of text 0x23 35 # 0x43 67 C 0x63 99 b 0x04 4 EOT End of transmission 0x24 36 0x44 68 D 0x64 100 d 0x05 5 ENQ Enquiry 0x25 37 % 0x45 69 E 0x65 101 e 0x06 6 ACK Acknowledge 0x26 38 & 0x46 70 F 0x65 101 e 0x07 7 BELL Bell 0x27 39 0x47 71 G 0x67 103 g 0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x66 102 10 10 10 10 10 10 10 10 10 <td>0x00</td> <td>0</td> <td></td> <td></td> <td>0x20</td> <td>32</td> <td>Space</td> <td>0x40</td> <td>64</td> <td>6</td> <td>0x60</td> <td>96</td> <td></td>	0x00	0			0x20	32	Space	0x40	64	6	0x60	96	
0x03 3 ETX End of text 0x23 35 # 0x43 67 C 0x63 99 c 0x04 4 EDT End of transmission 0x24 36 5 0x44 68 D 0x64 100 d 0x05 5 ENQ Enquiry 0x25 37 8 0x46 70 F 0x66 101 e 0x06 6 ACK Acknowledge 0x26 38 8 0x46 70 F 0x66 102 f 0x08 8 B Backspace 0x28 40 (0x48 27 H 0x66 104 h 0x09 9 T 0x66 104 h 0x49 73 I 0x66 104 h 0x00 12 x42 0x44 74 J 0x66 104 h 0x00 12 x47 0x44 74 J 0x66 104	0x01	1	SOH		0x21	33	1	0x41	65	Α	0x61	97	a
0x04 4 EOT End of transmission 0x24 36 \$ 0x44 68 D 0x64 100 d 0x05 5 ENQ Enquiry 0x25 37 \$ 0x45 69 E 0x65 101 d 0x06 6 ACK Acknowledge 0x26 38 \$ 0x46 70 F 0x66 102 f 0x07 7 BELL Bell 0x27 39 ' 0x47 71 G 0x67 103 g 0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x68 104 h 0x09 9 TAB Horizontal tab 0x29 41) 0x49 73 I 0x68 106 j 0x0B 1 VT Vertical tab 0x28 42 * 0x44 74 J 0x68 106 j 0x0C 12 FF Form Feed 0x2C 44 , 0x44 74 J 0x68 107 k 0x0D 13 CR Carriage return 0x2D 43 - 0x4D 77 M 0x6D 109 m 0x0F 15 SI Shift in 0x2E 46 - 0x4E 78 N 0x6E 110 n 0x10 16 DLE Data link escape 0x30 48 O 0x55 80 P 0x70 112 p 0x11 7 DC1 Device control 1 0x31 49 1 0x55 81 O 0x72 114 r 0x12 1 8 DC2 Device control 2 0x32 50 2 O 0x55 85 85 U O 0x72 114 r 0x12 1 8 DC2 Device control 3 0x33 51 3 Ox55 85 U Ox75 117 u 0x12 2 SVN Synchronous idle 0x36 54 6	0x02	2	STX		0x22	34		0x42	66	В	0x62	98	b
0x05 5 ENQ Enquiry 0x25 37 8 0x45 69 E 0x65 101 e 0x06 6 ACK Acknowledge 0x26 38 6 0x46 70 F 0x66 102 e 0x07 7 BELL Bell 11 0x27 39 0x46 70 F 0x66 102 g 0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x68 104 h 0x0A 10 F New line 0x22 41 0x49 73 I 0x69 105 16 16 10	0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	C
0x06 6 ACK Acknowledge 0x26 38 6 0x46 70 F 0x66 102 f 0x07 7 BELL Bell 0x27 39 0x47 71 G 0x67 103 6 104 71 0x68 104 4 0x48 72 H 0x68 104 4 0x48 72 H 0x68 104 4 0x48 73 I 0x69 105 i 0x08 11 Y Vertical tab 0x20 42 0x44 74 J 0x68 107 k 0x00 10 F Form Feed 0x20 45 - 0x40 77 M 0x60 109 m 0x00 13 C Carriage return 0x20 45 - 0x40 77 M 0x60 109 m 0x00 18 0x60 109 m 0x0	0×04	4	EOT		0x24	36	\$	0x44	68	D	0×64	100	d
0x07 7 BELL Bell 0x27 39 ' 0x47 71 G 0x67 103 g 0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x68 104) 0x48 72 H 0x68 104) 0x09 9 TAB Horizontal tab 0x29 41) 0x49 73 I 0x68 106) 0x69 105 i 0x0A 10 LF New line 0x2A 42 * 0x4A 74 J 0x66 106 j 0x6B 107 k 0x0B 11 VT Vertical tab 0x2B 43 + 0x4B 75 K 0x6B 107 k 0x6B 107 k 0x0C 12 FF Form Feed 0x2C 44 , 0x4C 76 L 0x6B 108 l 0x6B 107 k 0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6D 109 m 0x6D 109 m 0x0F 15 SI Shift in 0x2F 47 / 0x4F 79 0 0x6F 111 o 0x1D 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 p 0x10 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 p 0x11 17 Dc1 Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x12 18 DC2 Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x71 113 0x72 114 r 0x13 19 DC3 Device control 3 0x33 51 3 0x55 83 S 0x73 115 s 0x16 18 1 0x72 114 r 0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x16 18 1 0x75 117 u 0x15 2 I NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 2 2 SYN Synchronous idle 0x36 54 6 0x58 88 X 0x78 110 x 0x17	0x05	5	ENQ	Enquiry	0x25	37	ક	0x45	69	E	0x65	101	е
0x08 8 BS Backspace 0x28 40 (0x48 72 H 0x68 104 h 0x09 9 TAB Horizontal tab 0x29 41) 0x49 73 I 0x69 105 j 0x0B 11 VT Vertical tab 0x2B 43 + 0x4B 75 K 0x6B 107 k 0x0D 12 FF Form Feed 0x2C 44 , 0x4C 76 L 0x6D 10 0x6D 13 C 0x4B 77 M 0x6B 107 k 0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6B 100 m 0x0E 14 SO Shift out 0x2E 46 . 0x4E 78 N 0x6E 110 m 0x11 18 0x5E 46 . 0x4E	0x06				0x26	38	&	0x46	70	F	0x66	102	f
0x09 9 TAB Horizontal tab 0x29 41 0x49 73 I 0x69 105 i 0x0B 10 LF New line 0x2A 42 0x4A 74 J 0x6A 106 j 0x0B 11 V Vetical tab 0x2B 43 + 0x4B 75 K 0x6D 107 k 0x0C 12 FF Form Feed 0x2C 44 , 0x4C 76 L 0x6C 108 1 0x0E 14 S Shift out 0x2E 46 0x4E 78 N 0x6D 109 m 0x10 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 0x11 17 0x6F 11 0 0x10 18 10 0x71 113 0x6F 11 0x70 112 0x10 0x10 0x8 10	0x07	7	BELL	Bell	0x27	39	100	0x47	71	G	0x67	103	g
0x0A 10 LF New line 0x2A 42 * 0x4A 74 J 0x6A 106 j 0x0B 11 VT Vertical tab 0x2B 43 + 0x4B 75 K 0x6B 107 K 0x6B 107 K 0x6B 107 K 0x6C 108 1 0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6D 109 m 0x0F 15 SI Shift out 0x2E 46 - 0x4D 77 M 0x6D 109 m 0x10 16 DLE Data link escape 0x30 48 0 0x5D 80 P 0x70 112 p 0x11 17 DCI Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x12 18 DC2	0x08	8	BS		0x28	40	(0x48	72	H	0x68	104	h
0x0B 11 VT Vertical tab 0x2B 43 + 0x4B 75 K 0x6B 107 k 0x0C 12 FF Form Feed 0x2C 44 , 0x4C 76 L 0x6C 108 1 0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6D 109 m 0x0E 14 SO Shift out 0x2E 46 . 0x4E 78 N 0x6E 110 n 0x0F 15 SI Shift in 0x2F 47 / 0x4F 79 0 0x6F 111 o 0x10 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 p 0x11 17 DC1 Device control 1 0x31 49 1 0x51 81 0 0x71 113 q 0x12 18 DC2 Device control 2 0x22 50 2 0x52 82 R 0x72 114 r 0x13 19 DC3 Device control 3 0x33 51 3 0x53 83 0 0x73 115 s 0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x15 21 NAK Negative ack 0x36 54 6 0x56 86 V 0x76 118 v 0x17 23 ETB End transmission block 0x17 25 ETB End transmission block 0x37 55 7 0x57 8W 0x77 119 w 0x18 24 CAN Cancel 0x39 57 9 0x35 83 0x30 89 Y 0x79 121 y 0x1B 27 FSC Escape 0x3B 59 ; 0x5E 89 1 [0x76 122 c 0x1D 29 GS Group separator 0x3D 61 0x5E 94 0x76 126 - 0x1D 29 GS Group separator 0x3D 62 0x3E 62 > 0x5E 94 0x76 126 - 0x1D 29 GS Group separator 0x3B 62 > 0x5E 94 0x76 126 - 0x1D 29 GS Group separator 0x3B 62 > 0x5E 94 0x76 126 - 0x1D 29 GS Group separator 0x3B 62 > 0x5E 94 0x76 126 -	0x09	9	TAB		0x29	41)	0x49	73	I	0x69		i
0x0C 12 FF Form Feed 0x2C 44 , 0x4C 76 L 0x6C 108 1 0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6D 109 m 0x0E 14 SO Shift out 0x2E 46 0x4E 78 N 0x6D 109 m 0x0F 15 SI Shift in 0x2E 47 / 0x4F 79 0 0x6F 111 0 0x10 18 0x50 80 P 0x70 112 0x10 18 0x50 80 P 0x70 112 0x11 17 0c1 Device control 1 0x31 49 1 0x51 81 0 0x71 113 9 0x12 18 D2 0x72 114 r 0x12 18 0 0x71 113 9 0x52 82 R 0x72 <td>0x0A</td> <td>10</td> <td>LF</td> <td>New line</td> <td>0x2A</td> <td>42</td> <td>*</td> <td>0x4A</td> <td>74</td> <td>J</td> <td>0x6A</td> <td>106</td> <td>j</td>	0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0D 13 CR Carriage return 0x2D 45 - 0x4D 77 M 0x6D 109 m 0x0E 14 SO Shift out 0x2E 46 0x4E 78 N 0x6E 110 0x0F 15 0x4E 78 N 0x6E 111 0x0F 15 0x4E 78 N 0x6E 111 0x10 18 0x4E 78 N 0x6E 111 0x10 18 0x4E 78 N 0x6E 111 0x10 18 0x4E 78 N 0x6E 111 0x31 19 0x10 18 0x12 18 0x51 81 0x77 112 p 0x12 18 0x2 0x2 0x52 20 0x52 28 0x53 81 0x77 111 19 0x11 13 0x31 49 1 0x51 21 0x52 20 0x52 82 R 0x72	0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0E 14 SO Shift out 0x2E 46 . 0x4E 78 N 0x6E 110 n 0x0F 15 SI Shift in 0x2F 47 / 0x4F 79 0 0x6F 110 n 0x10 16 DLE Data Link escape 0x30 48 0 x50 80 P 0x70 112 p 0x11 17 DC1 Device control 2 0x32 50 2 0x52 82 R 0x71 113 q 0x13 19 DC3 Device control 3 0x33 51 3 0x53 83 S 0x72 114 r 0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x16 22 XYN Synchronous idle 0x35 53 5 0x56 86 V	$0 \times 0 C$	12	FF		0x2C	44	,	0x4C	76	L	0x6C	108	1
0x0F 15 SI Shift in 0x2F 47 / 0x4F 79 0 0x6F 111 0 0x10 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 0x11 17 Dc1 Device control 1 0x31 49 1 0x51 81 0 0x71 113 q 0x11 17 Dc1 Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x12 18 Dc2 Device control 3 0x33 51 3 0x53 83 S 0x73 115 q 0x14 20 Dc4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x15 21 NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x76 118 u 0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 119 w 0x18 24 CAN Cancel 0x38 56 8 0x58 88 X 0x78 120 x 0x19 25 EM End of medium 0x39 57 9 0x58 88 X 0x78 122 x 0x18 26 SUB Substitute 0x38 59 ; 0x58 91 (0x78 122 c 0x18 27 FSC Escape 0x38 59 ; 0x56 91 (0x78 122 c 0x10 28 FS File separator 0x10 RS Record separator 0x36 62 > 0x56 94 0x76 125 y 0x10 30 RS Record separator 0x38 62 > 0x56 94 0x76 125 y 0x18 30 RS Record separator 0x38 62 > 0x56 94 0x76 125 y 0x10 29 GS Group separator 0x38 62 > 0x56 94 0x76 125 y 0x10 29 RS Record separator 0x38 62 > 0x56 94 0x76 125 y 0x16 29 XB Substitute 0x38 61 = 0x50 93 1 0x76 125 y 0x10 29 RS Record separator 0x38 62 > 0x56 94 0x76 125 y 0x10 29 RS Record separator 0x38 62 > 0x56 94 0x76 125 y	0x0D	13	CR		0x2D	45	-	0x4D	77	M	0x6D	109	m
0x10 16 DLE Data link escape 0x30 48 0 0x50 80 P 0x70 112 p 0x11 17 DC1 Device control 1 0x31 49 1 0x51 81 0 0x71 112 p 0x12 18 Dc2 Device control 2 0x32 50 2 0x52 2 0x52 22 0x52 31 0x53 31 0x53 32 0x53 33 0x53 33 0x53 31 0x53 35 0x54 84 47 0x74 116 117 0x16 22 2xN 0x75 117 </td <td>0x0E</td> <td>14</td> <td>SO</td> <td></td> <td>0x2E</td> <td>46</td> <td></td> <td>0x4E</td> <td>78</td> <td>N</td> <td>0x6E</td> <td>110</td> <td>n</td>	0x0E	14	SO		0x2E	46		0x4E	78	N	0x6E	110	n
0x11 17 DC1 Device control 1 0x31 49 1 0x51 81 Q 0x71 113 q 0x12 18 DC2 Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x13 19 DC3 Device control 3 0x33 51 3 0x53 83 S 0x73 115 s 0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x16 21 NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x76 118 v 0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 <td< td=""><td>0x0F</td><td>15</td><td>SI</td><td></td><td></td><td>47</td><td>/</td><td></td><td></td><td>0</td><td>0x6F</td><td></td><td>0</td></td<>	0x0F	15	SI			47	/			0	0x6F		0
0x12 18 DC2 Device control 2 0x32 50 2 0x52 82 R 0x72 114 r 0x13 19 DC3 Device control 3 0x33 51 3 0x53 83 8 0x73 115 0x53 83 8 0x73 115 0x55 85 0x74 116 t 0x15 18 0x74 116 t 0x55 85 0 0x74 116 t 0x15 2x 0x55 85 0 0x74 116 t 0x16 2x 0x56 86 V 0x76 118 0x16 2x 0x56 86 V 0x76 118 0x19 2x 0x56 86 V 0x76 118 0x18 2x 0x76 117 0x55 87 W 0x77 119 W 0x18 2x 0x76 118 0x76 119 0x776 118 0x78 119	0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x13 19 DC3 Device control 3 0x33 51 3 0x53 83 S 0x73 115 s 0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 x 0x15 21 NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x76 118 v 0x18 24 CAN Cancel 0x38 56 80 x58 88 X 0x78 120 x 0x19 25 EM end of medium 0x39 57 9 0x59 89 Y 0x79 121 y 0x1B 26 SUB Substitute 0x38 59 ; 0x58 90 z 0x77 129 <td>0x11</td> <td>17</td> <td>DC1</td> <td>Device control 1</td> <td>0x31</td> <td>49</td> <td>1</td> <td>0x51</td> <td>81</td> <td>Q</td> <td>0x71</td> <td>113</td> <td>q</td>	0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x14 20 DC4 Device control 4 0x34 52 4 0x54 84 T 0x74 116 t 0x15 21 NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x75 118 v 0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 119 w 0x18 24 CAN Cancel 0x38 56 8 0x58 88 X 0x78 120 x 0x19 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 x 0x10 28 Substitute 0x38 59 ; 0x58 89 Y 0x77 122	0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0×72	114	r
0x15 21 NAK Negative ack 0x35 53 5 0x55 85 U 0x75 117 u 0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x76 118 V 0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 119 W 0x18 24 CAN Cancel 0x38 56 8 0x58 88 X 0x78 120 x 0x1D 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 y 0x1D 26 SUB Substitute 0x3B 59 ; 0x5B 99 2 0x79 121 y 0x1D 28 FS File separator 0x3C 60 <	0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	S
0x16 22 SYN Synchronous idle 0x36 54 6 0x56 86 V 0x76 118 v 0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 119 v 0x18 24 CAN Cancel 0x38 56 8 0x58 88 x 0x78 120 x 0x1D 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 y 0x1B 27 FSC Escape 0x38 58 : 0x5A 90 2 0x7A 122 y 0x1D 28 FS File separator 0x3C 60 <	0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x17 23 ETB End transmission block 0x37 55 7 0x57 87 W 0x77 119 w 0x18 24 CAN Cancel 0x38 56 8 0x58 88 X 0x78 120 x 0x19 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 y 0x1A 26 SUB Substitute 0x3A 58 : 0x5A 90 Z 0x7A 122 z 0x1D 27 FSC Escape 0x3B 59 ; 0x5B 91 [0x7B 123 { 0x1D 28 FS File separator 0x3C 60 0x5C 92 0x7C 124 0x1D 29 GS Group separator 0x3D 62 > 0x5E 94 ^ 0x7E 125 -	0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x18 24 CAN Cancel 0x38 56 8 0x58 88 X 0x78 120 x 0x19 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 y 0x1A 26 SUB Substitute 0x3A 58 0x5B 90 Z 0x7A 122 z 0x1B 27 FSC Escape 0x3B 59 ; 0x5B 91 [0x7B 123 4 0x1D 28 FS File separator 0x3B 60 0x5C 92 V 0x7C 124 1 0x1D 29 GS Group separator 0x3B 62 > 0x5E 93 1 0x7B 125 9 0x1E 30 RS Record separator 0x3E 62 > 0x5E 94 ^ 0x7E 125 +	0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x19 25 EM End of medium 0x39 57 9 0x59 89 Y 0x79 121 Y 0x1A 26 SUB Substitute 0x3A 58 : 0x5A 90 Z 0x7A 122 z 0x1B 27 FSC Escape 0x3B 59 ; 0x5B 91 (0x7B 123 q 0x1C 28 FS File separator 0x3C 60 0x5C 92 \ 0x7C 124 0x1D 29 GS Group separator 0x3B 62 > 0x5E 94 ^ 0x7E 126 - 0x1E 30 RS Record separator 0x3E 62 > 0x5E 94 ^ 0x7E 126 -	0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	W
0x1A 26 SUB Substitute 0x3A 58 : 0x5A 90 Z 0x7A 122 Z 0x1B 27 FSC Escape 0x1B 27 FSC Escape 0x3B 59 ; 0x5B 91 [0x7B 123 { 0x1C 28 FS File separator 0x1C 28 FS File separator 0x3C 60 < 0x5C 92 0x7C 124	0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x1B 27 FSC Escape 0x3B 59 ; 0x5B 91 [0x7B 123 { 0x1C 28 FS File separator 0x3C 60 0x5C 92 \ 0x7C 124 0x1D 29 GS Group separator 0x3D 61 = 0x5D 93] 0x7D 125) 0x1E 30 RS Record separator 0x3E 62 > 0x5E 94 ^ 0x7E 126 -	0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	У
0x1C 28 FS File separator 0x3C 60 < 0x5C 92 \ 0x7C 124	0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	\mathbf{z}	0x7A	122	Z
0x1D 29 GS Group separator	0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	1	0x7B	123	{
0x1E 30 RS Record separator	0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\ \	0x7C	124	
UXIE 30 KS RECOID SEPARACOI UXSE 02 > UXSE 94 UX/E 120	0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93]	0x7D	125	}
0x1F 31 US Unit separator	0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
	0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95		0x7F	127	DEL

Base64

- Shortest way to write binary as printable characters
- Common for keys and crypto
- This module will use Hex

Binary	ASCII
000000	Α
000001	В
000010	С
000011	D
000100	E
000101	F
000110	G
000111	Н
001000	1
001001	J
001010	K
001011	L
001100	М
001101	N
001110	0
001111	Р

Binary	ASCII
010000	Q
010001	R
010010	S
010011	Т
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z
011010	а
011011	b
011100	С
011101	d
011110	e
011111	f

Binary	ASCII
100000	g
100001	h
100010	į
100011	j
100100	k
100101	- 1
100110	m
100111	n
101000	0
101001	р
101010	q
101011	r
101100	S
101101	t
101110	u
101111	V

Binary	ASCII
110000	W
110001	х
110010	У
110011	Z
110100	0
110101	1
110110	2
110111	3
111000	4
111001	5
111010	6
111011	7
111100	8
111101	9
111110	+
111111	/

Code Demos

See Recording.

Caesar Cipher

- One of the first ciphers was used by Julius Caesar.
- The Caesar Cipher replaces each letter of the alphabet with one three to the right, i.e.
 - a becomes d
 - b becomes e
 - . . .
 - z becomes c.

Using a Key

 These ciphers are easy to break because as soon as you know the scheme you can decrypt the message.

Kerckhoffs' principle: A cipher should be secure even if the attacker knows everything about it apart from the key.

 \bullet For instance, we can use the Caesar cipher using n rotations.

VIGENERE TABEL

PLAIN TEXT

A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Y Z A B C D C B F G H I J K L M N O P Q R S T U V W X Y Z A B C D C B F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J												EVI	114 1	PLA												
B B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J X K L M N O P Q R S T U V W X Y Z A B C D E F G H	X Y Z	Х	W	٧	U	Т	S	R	Q	Р	0	N	М	L	K	J	1	Н	G	F	Е	D	С	В	Α	
C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J X K L M N O P Q R S T U V W X Y Z A B C D E F G H I J X K L M N O P Q R S T U V W X Y Z A B C D E F G H I J X K L M N O P Q R S T U V W X Y Z A B C D E F G M I J X Y Z A B C D E F G M I J X Y Z A B C D E F G M I J X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X Y Z A B C D E F G M I J X X X X X X X X X X X X X X X X X X	X Y Z	X	W	٧	U	Т	S	R	Q	Р	0	Ν	M	L	K	J	1	Н	G	F	Е	D	C	В	Α	Α
D D E F G H I J J K L M N O P Q R S T U V W X Y Z A B G G G H I J J K L M N O P Q R S T U V W X Y Z A B G G G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T W V W X Y Z A B C D E F G M I J J K L M N O P Q R S T W V W X Y Z A B C D E F G M I J J K L M N O P Q R S T W V W X Y Z A B C D E F G M I J J K L M N O P Q R S T W X Y Z A B C D E F G M I J J K L M N O P Q R S T W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L M N O P Q R S T U V W X Y Z A B C D E F G M I J J K L	YZA	Υ	X	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	D	С	В	В
E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F	Z A B	Z	Υ	X	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	D	С	С
F F G H I J J K L M N O P Q R S T U V W X Y Z A B C D H H I J K L M N O P Q R S T U V W X Y Z A B C D H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O R R S T U V W X Y Z A B C D E F G H I J K L M N O R C S S T U V W X Y Z A B C D E F G H I J K L M N O R C S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q	A B C	Α	Z	Υ	X	W	٧	U	Т	S	R	Q	Р	0	N	М	L	K	J	1	Н	G	F	Ε	D	D
G G H I I J K L M N O P Q R S T U V W X Y Z A B C D E I G H I I J K L M N O P Q R S T W W X Y Z A B C D E I G H I I J K L M N O P Q R S T U V W X Y Z A B C D E I G H I I J K L M N O P Q R S T W W X Y Z A B C D E I G H I I J K L M N O P Q R S T W W X Y Z A B C D E I G H I I J K L M N O P Q R S T W W X Y Z A B C D E I G H I I J K L M N O P Q R S T W X X Y Z A B C D E I G H I I J K L M N O P Q R S T W X X Y Z A B C D E I G H I I J K L M N O P Q R S T W X X Y Z A B C D E I G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U V W X X Y Z A B C D E I F G H I I J K L M N O P Q R S T U	B C D	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	E
H H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U X X Y Z A B C D E F G H I J J K L M N O P Q R S T U X X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N	C D E	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	F
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J J K L M N O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O O P Q R S T U V W X Y Z A B C D E F G H L J K L M N O O P Q R S T U V V W X Y Z A B C D E F	D E F	D	С	В	Α	Z	Υ	X	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	L	Н	G	G
J J K L M N O P Q R S T U V W X Y Z A B C D E F G H S T U V W X Y Z A B C D E F G H I J V W X Y Z A B C D E F G H I J K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N D V W X Y Z A B C D E F G H I J K	E F G	Е	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	Н
K K L M N O P Q R S T U V W X Y Z A B C D E F G H I M N O P Q R S T U V W X Y Z A B C D E F G H I M N O P Q R S T U V W X Y Z A B C D E F G H I M N O P Q R S T U V W X Y Z A B C D E F G H I M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X Y Y Z A B C D E F G H I J J K L M N O P Q R S T U X	F G F	F	Ε	D	С	В	Α	Z	Υ	X	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	1
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O Q Q R S T U V W X Y Z A B C D E F G H I J K L N O Q Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S W W X Y Z A B C D E F G H I J K L N N O P Q R S T U Y W X Y Z A B C D E F G H I J K L N N O P Q R S T U Y W X Y Z A B C D E F G H I J K L N N O P Q R S T U Y W X Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L N N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L N N O P Q R S T U Y Y Y Z A B C D E F G M I J J K L N N O P Q R S T U Y Y Y Z A B C D E F G M I J J K L N N O P Q R S T U Y Y Y Z A B C D D E F G M I J J K L N N O P Q R S T U Y Y Y Z A B	G H I	G	F	Е	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	М	L	K	J	J
M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U Y W X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E	H I J	Н	G	F	Ε	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	К
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J J K L P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T W W X Y Z A B C D E F G H I J K L M N O P Q R S T W W X Y Z A B C D E F G H I J K L M N O P Q R S T W W X Y Z A B C D E F G H I J K L M N O P Q R S T W W X Y Z A B C D E F G H I J K L M N O P Q R S T W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U Y X X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G H I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R S T U W Y Y Z A B C D E F G M I J J K L M N O P Q R	I J K	I	Н	G	F	Е	D	С	В	Α	Z	Υ	Х	W	٧	U	Т	S	R	Q	Р	0	N	M	L	L
O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y	J K L	J	1	Н	G	F	Е	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	M	М
P P Q R S T U V W X Y Z A B C D E F G H I J K L M N Q Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P S S T U V W X Y Z A B C D E F G H I J K L M N O P Q T T U V W X Y Z A B C D E F G H I J K L M N O P Q	K L N	K	J	1	Н	G	F	Е	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	N	N
Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O S S T U V W X Y Z A B C D E F G H I J K L M N O P Q U U V W X Y Z A B C D E F G H I J K L M N O P Q U U V W X Y Z A B C D E F G H I J K L M N O P Q U U V W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y X Z A B C D E F G H I J K L M N O P Q R S T U V Y X Z A B C D E F G H I J K L M N O P Q R S T U V Y Y Z A B C D E F G H I J J K L M N O P Q R S T U V Y	L M N	L	K	J	1	Н	G	F	Е	D	C	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	0	0
R R S T U V W X Y Z A B C D E F G H I J K L M N O P T U V W X Y Z A B C D E F G H I J K L M N O P T T U V W X Y Z A B C D E F G H I J K L M N O P T T U V W X Y Z A B C D E F G H I J K L M N O P Q R V W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S T W X X Y Z A B C D E F G H I J K L M N O P Q R S T W X X Y Z A B C D E F G H I J K L M N O P Q R S T W X X Y Z A B C D E F G H I J K L M N O P Q R S T U V Y Z A B C D E F G H I J K L M N O P Q R S T U V Y Y Z A B C D E F G H I J K L M N O P Q R S T U V Y	M N C	M	L	K	J	T	Н	G	F	Е	D	С	В	Α	Z	Υ	Χ	W	٧	U	Т	S	R	Q	Р	Р
S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S X Y Z A B C D E F G H I J K L M N O P Q R S X X Y Z A B C D E F G H I J K L M N O P Q R S X X Y Z A B C D E F G H I J K L M N O P Q R S T X X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y X X Z A B C D E F G H I J K L M N O P Q R S T U Y X X X Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y	N O P	N	М	L	K	J	T	Н	G	F	E	D	С	В	Α	Z	Υ	X	W	٧	U	Т	S	R	Q	Q
T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W X Y Z A B C D E F G H I J K L M N O P Q R S W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Z A B C D E F G H I J K L M N O P Q R S T U Y Z A B C D E F G H I J K L M N O P Q R S T U Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y	O P C	0	N	M	L	K	J	T	Н	G	F	Е	D	С	В	Α	Z	Υ	X	W	٧	U	Т	S	R	R
U U V W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S W W X Y Z A B C D E F G H I J K L M N O P Q R S T X X X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U Y	P Q R	Р	0	N	M	L	K	J	1	Н	G	F	E	D	С	В	Α	Z	Υ	X	W	٧	U	Т	S	S
V V W X Y Z A B C D E F G H I J J K L M N O P Q R S W W X Y Z A B C D E F G H I J J K L M N O P Q R S T X X Y Z A B C D E F G H I J J K L M N O P Q R S T U Y Y Z A B C D E F G H I J J K L M N O P Q R S T U V	Q R S	Q	Р	0	N	М	L	K	J	1	Н	G	F	Е	D	С	В	Α	Z	Υ	X	W	٧	U	Т	Т
W W X Y Z A B C D E F G H I J K L M N O P Q R S T X X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U V	R S T	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	D	С	В	Α	Z	Υ	X	W	٧	U	U
X X Y Z A B C D E F G H I J K L M N O P Q R S T U Y Y Z A B C D E F G H I J K L M N O P Q R S T U V	STL	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	D	C	В	Α	Z	Υ	X	W	٧	٧
Y Y Z A B C D E F G H I J K L M N O P Q R S T U V	T U V	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	Е	D	С	В	Α	Z	Υ	Χ	W	W
	UVV	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	E	D	С	В	Α	Z	Υ	X	Х
Z Z A B C D E F G H I J K L M N O P Q R S T U V W	V W X	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	L	Н	G	F	Е	D	С	В	Α	Z	Υ	Υ
	WXY	W	٧	U	Т	S	R	Q	Р	0	N	M	L	K	J	1	Н	G	F	E	D	С	В	Α	Z	Z

VIGENERE TABEL

ΡΙ ΔΙΝ ΤΕΧΤ

												PLA	IIV I	EVI												
	Α	В	С	D	Ε	F	G	Н	1	J	K	L	M	Ν	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
Α	Α	В	С	D	Е	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z
В	В	С	D	Е	F	G	Ξ	1	J	K	L	Μ	Z	0	P	Q	R	S	Т	J	٧	W	X	Υ	Z	Α
С	С	D	Ε	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В
D	D	Ε	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С
Ε	Ε	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D
F	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	E
G	G	Н	1	J	K	L	M	N	0	P	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	C	D	Е	F
Н	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	C	D	E	F	G
1	1	J	K	L	M	Z	0	Р	Q	R	S	Т	٥	٧	W	X	Υ	Z	Α	В	C	D	E	F	G	Н
J	J	K	L	M	Ν	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1
K	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Y	Z	Α	В	С	D	E	F	G	Н	1	J
L	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K
M	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L
N	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	M
0	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	C	D	Е	F	G	Н	1	J	K	L	M	N
Р	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	M	N	0
Q	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	M	N	0	Р
R	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	T	J	K	L	M	N	0	Р	Q
S	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	M	N	0	Р	Q	R
T	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S
U	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т
٧	٧	W	Χ	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U
W	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧
Х	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	T	U	٧	W
Υ	Υ	Z	Α	В	С	D	Е	F	G	Н	L	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ
Z	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ

KEY

Caesar

VIGENERE TABEL

TENE TABLE

													PLA	IN T	EXT												
		Α	В	С	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	T	U	٧	W	Х	Υ	Z
	Α	Α	В	С	D	E	F	G	Н	-	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z
	В	В	С	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α
	С	С	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В
	D	D	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С
	E	Е	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D
	F	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е
	G	G	Н	-	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F
	Н	Н	L	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	E	F	G
	ı	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н
	J	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н	1
	K	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н	1	J
	L		М	N	0	Р	0	R	S	Т	U	V	W	X	Υ	Z	Α	В	С	D	Е	F	G	н	1	J	K
	- 1	-			_		ч		_		_	•	•••	,,		_		_	_	_	_		_			_	
- 1-	М	М	N	0	Р	Q	R	S	T	U	٧	W	Х	Υ	Z	A	В	С	D	E	F	G	Н	1	J	K	L
2	-	M			_		_		T		V	-		Y		_		C	_	_	_		_	J	J	K	L M
2	М		N	O P Q	P Q R	Q R S	R S T	S T U	Т	U	V W	W X Y		Υ	Z	Α	B C D	_	D	E F G	F	G	H	J K	J K L	K L M	L
	M N	N	N O	O P	P	Q R	R S T U	S	T U V	V	V	X	X	Y	Z	A	В	D	D	E F	F	G	_	J	J K L	L	M N O
	M N O	N O	N O P	O P Q R	P Q R	Q R S T U	R S T U	S T U	T U V	V W X Y	V W	W X Y	X Y Z A B	Y Z A	Z A B C	A B C D	B C D E	D E F	D E F	E F	F G H	G H	H	J K	J K L M	M N O	L M N
	M N O P Q R	N O P Q R	N O P Q R	O P Q R S	P Q R S T	Q R S T U	R S T U V	S T U V W	T U V W X	V W X Y	V W X Y Z A	X Y Z A B	X Y Z A B	Y Z A B C	Z A B C D	A B C D E	B C D E F	D E F	E F G H	F G H	F G H	G H J K L	H J K L	J K L M	N O	L M N O	M N O P
	M N O P	N O P Q	N O P Q R	O P Q R	P Q R S	Q R S T U	R S T U	S T U V	T U V W	V W X Y	V W X Y	W X Y Z A	X Y Z A B	Y Z A B	Z A B C	A B C D	B C D E	D E F	D E F G	F G H	F G H I	G H I J	H J K L	J K L	N	M N O	M N O P Q R
	M N O P Q R	N O P Q R	N O P Q R S T	O P Q R S T U V	P Q R S T	Q R S T U	R S T U V W X Y	S T U V W	T U V W X	V V X Y Z A B	V W X Y Z A	X Y Z A B	X Y Z A B C D	Y Z A B C D E F	Z A B C D E F	A B C D E	B C D E F	D E F G	E F G H	F G H	F G H I J	G H J K L	H J K L	J K L M	N O	L M N O P Q R	L M N O P Q R
	M N O P Q R S T	N O P Q R S T	N O P Q R S T U	O P Q R S T U V W	P Q R S T U V W X	Q R S T U V W X	R S T U V W X Y	S T V V X Y Z A	T V W X Y Z A B	V W X Y Z A B	V W X Y Z A B C	W X Y Z A B C D	X Y Z A B C D	Y Z A B C D E F G	Z A B C D E	A B C D E F	B C D E F G H I	D E F G H	D F G H J	E F G H J K L	F G H J K L	Б Н Г К К В О	H J K L M	K L M N O P	N O P Q R	L M N O P Q R	M N O P Q R S
	M N O P Q R S T U	N O P Q R S T U	N O P Q R S T U V	O P Q R S T U V W X	P Q R S T U V W X Y	Q R S T U V W X Y Z	R S T U V W X Y Z A	S T U V W X Y Z A B	T V W X Y Z A B	V W X Y Z A B C	V X Y Z A B C D	W X Y Z A B C D E F	X Y Z A B C D E F	Y Z A B C D E F	Z A B C D E F	A B C D E F G H	B C D E F G H	D E F G H I J K L	D E F G H I K L	F G H J K L M	F G H I J K L M Z O	H J K L M N O P	H J K L M N O P	K L M N O P Q R	N O P Q R	M N O P Q R S	M N O P Q R S T
	M N O P Q R S T U	N O P Q R S T U V	N O P Q R S T U V	O P Q R S T U V W X Y	P Q R S T U V W X	Q R S T U V W X Y Z	R S T U V W X Y Z A B	S T V V X Y Z A	T U V W X Y Z A B C	V W X Y Z A B C D	V W X Y Z A B C D E	W X Y Z A B C D E F	X Y Z A B C D	Y Z A B C D E F G	A B C D E F G H	A B C D E F G H	B C D E F G H I	D E F G H J K L	D E F G H - J K	F G H I J K L M N O	F G H J K L M	G H J K L M N O P	H I J K L M N O P Q R	J K L M N O P Q R	N O P Q R S	M N O P Q R S T	M N O P Q R S T U
	M N O P Q R S T U V	N O P Q R S T U	N O P Q R S T U V	O P Q R S T U V W X	P Q R S T U V W X Y	Q R S T U V W X Y Z	R S T U V W X Y Z A	S T U V W X Y Z A B C D	T V W X Y Z A B	V W X Y Z A B C	V W X Y Z A B C D E F	W X Y Z A B C D E F	X Y Z A B C D E F	Y Z A B C D E F G H	A B C D E F G	A B C D E F G H	B C D E F G H I J	D E F G H I J K L	E F G H J K L M	F G H J K L M	F G H J K L M N O P	H J K L M N O P	H I J K L M N O P Q R S	K L M N O P Q R	N O P Q R S T	M N O P Q R S T U	M N O P Q R S T U V
	M N O P Q R S T U	N O P Q R S T U V	N O P Q R S T U V	O P Q R S T U V W X Y	P Q R S T U V W X Y Z	Q R S T U V W X Y Z	R S T U V W X Y Z A B	S T U V W X Y Z A B	T U V W X Y Z A B C	V W X Y Z A B C D	V W X Y Z A B C D E	W X Y Z A B C D E F	X Y Z A B C D E F G	Y Z A B C D E F G H I	A B C D E F G H	B C D E F G H I J K	B C D E F G H I J K	D E F G H J K L	E F G H J K L	F G H I J K L M N O	F G H I J K L M N O P	G H J K L M N O P	H I J K L M N O P Q R	J K L M N O P Q R	N O P Q R S	M N O P Q R S T	M N O P Q R S T U

Rot 13

Using a Key

- For instance, we can use the Caesar cipher with *n* rotations
- But only 26 possible keys so you can just try them all (breaking the cipher is 26 times harder without the key)

Using a Key

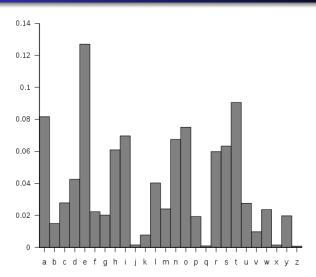
- For instance, we can use the Caesar cipher with *n* rotations
- But only 26 possible keys so you can just try them all (breaking the cipher is 26 times harder without the key)
- A better scheme replaces each letter with another letter. Here there are 26! $\approx 4 \cdot 10^{26}$ possible keys.

Frequency Analysis

- While hard to break by brute force, replacing each letter with another is easy to break using frequency analysis.
- •
- Frequency analysis counts the number of times
 - each symbol occurs
 - each pair of symbols
 - etc.

and tries to draw conclusions from this.

Frequency Analysis



Summary

- Code is any binary representation of data; cipher is a code where it is difficult to derive data from code.
- Looked at various codes, including Hex
- Looked at substitution ciphers, which replace single letters. These are easily breakable.

Symmetric Cryptography

Overview

- Will now look at proper encryption schemes
- Assumption: All participants share common secret key (obviously problematic!)
- Will consider most important encryption schemes and possible attacks against them
- Need some mathematical prerequisites to explain encryption schemes (modular arithmetic)

Modular Arithmetic

- ullet Arithmetic modulo n means that you count up to n-1 then loop back to 0
- i.e., $0, 1, 2, \ldots, n-1, 0, 1, 2, \ldots, n-1, 0, 1, 2, \ldots$
- $a \mod b = r$ for largest whole number k such that a = b * k + r
- e.g. $9 \mod 4 = 1$ because 9 = 2 * 4 + 1

• xor (\oplus) is binary addition modulo 2:

$$\begin{array}{rcl}
0 \oplus 0 & = & 0 \\
1 \oplus 0 & = & 1 \\
0 \oplus 1 & = & 1 \\
1 \oplus 1 & = & 0
\end{array}$$

- xor on bitstrings of same length defined by applying xor to corresponding bits
- Important properties
 - xor is associative and commutative
 - for all bitstrings M, $M \oplus 0 = M$
 - for all bitstrings M, $M \oplus M = 0$

where 0 is a bitstring of all 0's of the appropriate length

• Needs a key as long as the message.

Message: HELLOALICE

Key:

Cipher text:

• Needs a key as long as the message.

Message: HELLOALICE Key: THFLQRZFJK

Cipher text:

- Needs a key as long as the message.
- XOR/add the key and the message: (Demonstrated here with strings and addition and subtraction of keys; for bitstrings use xor)

Message: HELLOALICE Key: THFLQRZFJK Cipher text: ALRWERKNLO

• Needs a key as long as the message.

Cipher text: ALRWERKNLO

Key:

Plain text:

• Needs a key as long as the message.

Cipher text : ALRWERKNLO Key: THFLQRZFJK

Plain text:

- Needs a key as long as the message.
- XOR/add the key and the message: (Demonstrated here with strings and addition and subtraction of keys; for bitstrings use xor)

Cipher text : ALRWERKNLO
Key: THFLQRZFJK
Plain text: HELLOALICE

• Needs a key as long as the message.

Cipher text: ALRWERKNLO

Key:

Plain text:

• Needs a key as long as the message.

Cipher text : ALRWERKNLO Key: UXDTDXFHXN

Plain text:

- Needs a key as long as the message.
- XOR/add the key and the message: (Demonstrated here with strings and addition and subtraction of keys; for bitstrings use xor)

Cipher text : ALRWERKNLO Key: UXDTDXFHXN Plain text: GOODBYEBOB

Have perfect encryption:

You don't learn anything about the plaintext from the ciphertext

Theorem

Given any ciphertext of a certain length, without knowing the key the probability of the ciphertext being the encryption of a plaintext of the same length is the same for all plaintexts of the same length as the ciphertext.

- Problem
 - The key needs to be as long as the message
 - Must use key only once
- Russia during and after WW2
 - Reused the key material (ie encrypted several messages with the same key)
 - Broken by the Venona project

Block Ciphers

- Modern ciphers work on blocks of plain text, not just a single symbol.
- They are made up of a series of permutations and substitutions repeated on each block.
- The key controls the exact nature of the permutations and substitutions

Advanced Encryption Standard (AES)

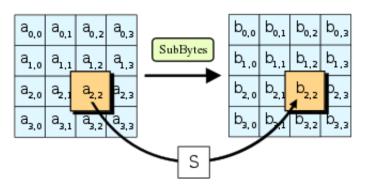
- AES is a state-of-the-art block cipher.
- It works on blocks of 128-bits.
- It generates 10 round keys from a single 128-bit key.
- It uses one permutation: *ShiftRows* and three substitutions *SubBytes*, *MixColumns*, *AddRoundKey*.

Advanced Encryption Standard (AES)

A block of 128 bits is represented by a 4×4 -matrix where each matrix element is a byte (8 bits), written as

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

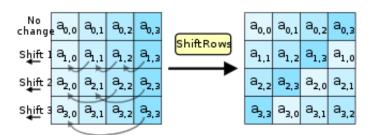
SubBytes: S-box



from Wikipedia

SubByte is an operation on bytes using finite field arithmetic

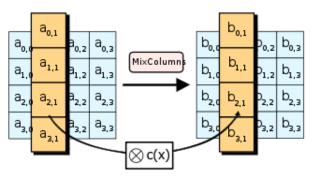
ShiftRows



from Wikipedia

- ShiftRows moves the
 - 2nd row one byte to the left,
 - the 3rd row two bytes
 - and the 4th row 3 bytes.

MixColumn

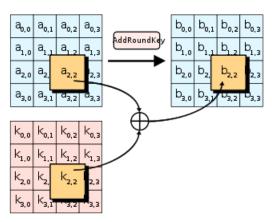


from Wikipedia

MixColumn is a substitution of each column such that:

$$(a_0x^3 + a_1x^2 + a_2x + a_3) \times (3x^3 + x^2 + x + 2) \mod(x^4 + 1) = (b_0x^3 + b_1x^2 + b_2x + b_3)$$

AddRoundKey



from Wikipedia

AddRoundKey applies \oplus to the block and the 128-bit round key (which was generated from the main key).

Security of AES

- No formal proof of security (P = NP?) but best known cryptographic attack requires 2^{126} key guesses an (irrelevant) improvement of factor 4 compared to 2^{128} key guesses via brute force attack
- There are side channel attacks (eg via measuring power consumption, execution time) — see later in the course.
- Key aspects of security:
 - Shuffling of rows and columns to ensure small change in input causes very big change in output
 - Require at least one non-linear operation (in the sense of linear algebra) on the data provided by the *SubByte*-operation

DES

- The Data Encryption Standard (DES), was the previous standard.
- Designed by IBM in early 1970's
- Before it was accepted as a standard the NSA stepped in and added S-boxes and fixed the key length at 56 bits

DES

- S-boxes are a type of substitution.
- It was unclear at the time why the NSA added S-boxes to the design.
- Many believed these were a back door for the NSA.

DES

- In 1990, Biham and Shamir discovered differential cryptanalysis.
- The S-boxes had made DES resistant to differential cryptanalysis.
- It seems that the NSA knew about differential cryptanalysis, at the start of the 1970s and had step into to protect DES.

Cost to Break DES

- 1977, Diffie and Hellman, theoretically: \$20 million, break in 1 day.
- 1993, theoretically \$1 million, in 7 hours.
- 1997, RSA Security offer \$10,000 for a real break, won by a distributed computing project, at "no cost"
- EFF (Electronic rights group) break in 56 hours for \$250,000
- 2006, COPACOBANA, general purpose brute force, break DES for \$10,000
- 2016, hashcat on Nvidia GeForce GTX 1080 Ti GPU costing \$1000 USD recovers a key in an average of 15 days

A word about key length



ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.

DRUG HIM AND HIT HIM WITH

THIS \$5 WRENCH UNTIL

HE TELLS US THE PASSWORD.

GOT IT.

Source: https://xkcd.com/538/

3-DES

- Triple DES, was a stop gap until AES
- 3-DES takes 3 keys, k_1 , k_2 and k_3 .

$$E_{k_1,k_2,k_3}(M) = E_{k_3}(D_{k_2}(E_{k_1}(M)))$$

- Setting $k_1 = k_2 = k_3$ gives you DES
- Expected to be good until 2030
- Used in bank cards and RFID chips

- Block ciphers only work on fixed size blocks.
- If the message isn't of the right block size we need to pad the message.
- But receiver needs to tell the difference between the padding and message.

• Add random bytes to the end of the block?

• Add random bytes to the end of the block? No.

- Add random bytes to the end of the block? No.
- Add zeros to the end of the block?

- Add random bytes to the end of the block? No.
- Add zeros to the end of the block? No.

- Add random bytes to the end of the block? No.
- Add zeros to the end of the block? No.
- Write "this is padding"?

- Add random bytes to the end of the block? No.
- Add zeros to the end of the block? No.
- Write "this is padding"? No.

Padding: PKCS 5/7

- If there is 1 byte of space write 01
- If there are 2 byte of space write 0202
- If there are 3 byte of space write 030303
- ...
- If the message goes to the end of the block add a new block of 16161616..

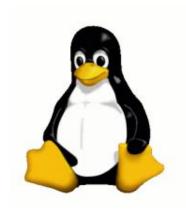
PKCS 7: 16 byte block, PKCS 5: 8 byte block

- Block Ciphers can be used in a number of modes:
 - Electronic codebook mode (ECB)
 - each block is encrypted individually,
 - encrypted blocks are assembled in the same order as the plain text blocks.
 - if blocks are repeated in the plain text, this is revealed by the cipher text.

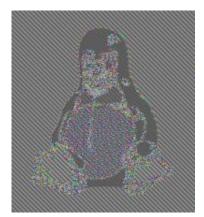
Demo Block Problems



Original



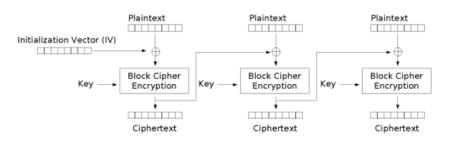




I ECB

Source: Wikipedia

- 2 Cipher Block Chaining Mode (CBC)
 - each block XOR'd with previous block
 - start with a random Initialization Vector (IV)
 - helps overcome replay attack.
 - Suppose the plain text is B_1, B_2, \ldots, B_n . IV = random number (sent in the clear) C_1 = $encrypt(B_1 \oplus IV)$ C_2 = $encrypt(B_2 \oplus C_1)$ \ldots C_n = $encrypt(B_n \oplus C_{n-1})$



Cipher Block Chaining (CBC) mode encryption

Source: Wikipedia

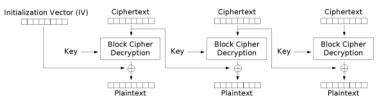
CBC decrypt

- Receive IV
- Receive cipher text C_1, C_2, \ldots, C_n
- Plain text is B_1, B_2, \ldots, B_n , where

$$B_1 = decrypt(C_1) \oplus IV$$

 $B_2 = decrypt(C_2) \oplus C_1$
...
 $B_n = decrypt(C_n) \oplus C_{n-1}$

CBC decrypt

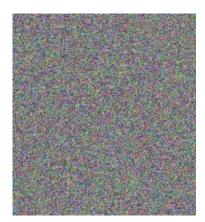


Cipher Block Chaining (CBC) mode decryption

Source: Wikipedia







CBC

Source: Wikipedia

Probabilistic Encryption

- Probabilistic encryption schemes use random elements to make every encryption different.
- CBC with a random IV is a good way to make encryption probabilistic.
- Using CBC and random IVs lets me encrypt the same message, and with the same key, without an attacker realising.

Misuse of IV

IV must be random, different for each encrypted block

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
    // guaranteed to be random.
}
```

https://xkcd.com/221

Choosing fixed IV can have devastating effect (Zerologon vulnerability for Microsoft Windows (https://www.secura.com/pathtoimg.php?id=2055))

Zerologon

- Windows has RPC for updating password on the domain controller
- Uses cryptographic protocols for authenticating these requests
- In particular, use AES with block cipher mode called CFB8, which uses IV exactly as CBC mode.
- This is secure with randomly chosen IV
- Implementation chooses IV to be always 0

Zerologon

- Consequence: AES-CFB8 encryption on all-zero plaintext will produce all-zero ciphertext
- This can be used to bypass authentication completely and set domain controller password
- Attack only requires network access to domain controller, which is available from any machine in the domain
- CVSS score of 10.0
- Department of Homeland Security forced all US government institutions to patch Windows Servers within three days

Sony PlayStation

- Sony needs to stop games being copied.
- CD and full disk encryption
- User can read and write areas of the hard disk, for own files, notes, etc
- Why won't CBC work?



Sony PlayStation

- With CBC, you need to encrypt, or decrypt, the whole file to get to the end.
- The Sony PlayStation uses ECB full disk encryption, to stop people copying games.
- User can access files they made themselves
- Hardware controls user access to data.



Sony PlayStation Disk Encryption Attack

- Remove disk and make copy
- 2 Replace disk in Playstation.

Sony PlayStation Disk Encryption Attack

- Remove disk and make copy
- Replace disk in Playstation.
- Copy a file to the disk
- Remove disk and find the bit of disk that changed (this is the encrypted file)



Sony Play Station Disk Encryption Attack

Opp target data to user area

Sony PlayStation Disk Encryption Attack

- Oppy target data to user area
- Restart the PlayStation and ask for your file back
- PlayStation decrypts the file and gives you back the plain text



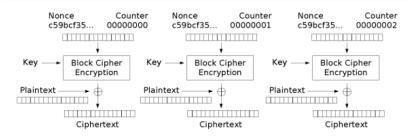
Counter Mode (CTR)

- Plain text: B_1, B_2, \ldots, B_n
- IV: random number (sent in clear)
- Cipher text: C_1, C_2, \ldots, C_n where

$$C_1 = B_1 \oplus encrypt(IV)$$

 $C_2 = B_2 \oplus encrypt(IV + 1)$
...
 $C_n = B_n \oplus encrypt(IV + n - 1)$

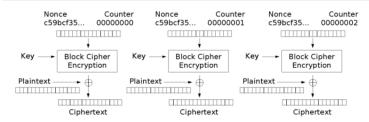
Counter Mode (CTR)



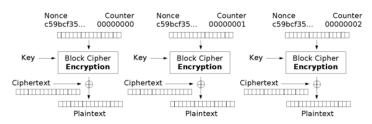
Counter (CTR) mode encryption

Source: Wikipedia

Counter Mode (CTR)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Cipher Texts Can Be Altered

- AES encryption with a particular key maps any 128-bit block to a 128-bit block (or 256)
- AES decrypt also maps any 128-bit block to a 128-bit block.
- Decrypt can be run on any block (not just encryptions).

- If I know the plaintext I can change CTR encrypted messages
- eg If I know $Enc_{CTR}(M_1)$ and I know M_1 , I can make a ciphertext that decrypts to any message I want, eg M_2
- New ciphertext is

$$Enc_{CTR}(M_1) \oplus (M_1 \oplus M_2)$$

Decrypt it:

$$Dec_{CTR}(Enc_{CTR}(M_1) \oplus (M_1 \oplus M_2)) =$$

Decrypt it:

$$Dec_{CTR}(Enc_{CTR}(M_1) \oplus (M_1 \oplus M_2)) = Dec_{CTR}(Enc(N||Ctr) \oplus M_1) \oplus (M_1 \oplus M_2) =$$

Decrypt it:

```
Dec_{CTR}(Enc_{CTR}(M_1) \oplus (M_1 \oplus M_2)) = \\ Dec_{CTR}(Enc(N||Ctr) \oplus M_1) \oplus (M_1 \oplus M_2) = \\ Enc(N||Ctr) \oplus (Enc(N||Ctr) \oplus M_1) \oplus (M_1 \oplus M_2) = \\ M_2
```

Have to stop this Subject of future lecture

Summary

- Introduced symmetric encryption. Assumption: All participants share common secret key.
- One-time pad provides perfect encryption (no attack possible), but requires key as long as message.
- Discussed DES and AES algorithms for symmetric encryption of one block
- Discussed block cipher modes (ECB, CTR, CCB) for encryption of several blocks
- Cryptographic schemes are brittle: small errors give rise to attacks. Some examples were given.