Mathematics 124 (Winter 2009)
Binary One-Time Pad

Recall the addition modulo 2 table is given by

+	0	1
0	0	1
1	1	0

Exercise. Determine the subtraction modulo 2 table:

−	0	1
0		
1		

Example. Suppose that the key is

11011101 11111011 10010011 01110000.

Encipher the plaintext `PLAN` using the binary Vigenère cipher.

Solution. The ASCII codes for `PLAN` are 80 76 65 78 which converted to binary gives

plain	01010000	01001100	01000001	01001110
key	11011101	11111011	10010011	01110000
cipher	10001101	10110111	11010010	00111110

The ciphertext in decimal is 141 183 210 62.

Example. Decipher

10010101 10111110 11011111 00100000

which was enciphered with the key

11011101 11111011 10010011 01110000

and interpret the results as four ASCII values.

Solution. Adding bits modulo 2, we find

cipher	10010101	10111110	11011111	00100000
key	11011101	11111011	10010011	01110000
plain	01001000	01000101	01001100	01010000
decimal	72	69	76	80

and so the decoded ASCII plaintext is `HELP`.