Cryptography

Robin Whitty

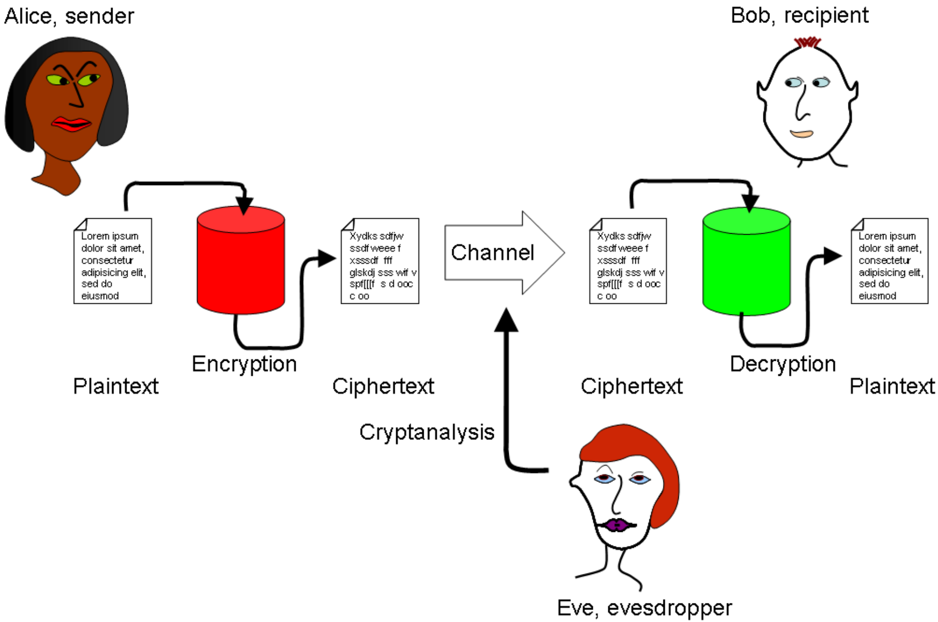
London South Bank University

Touring Turing, Rewley House, July 2012

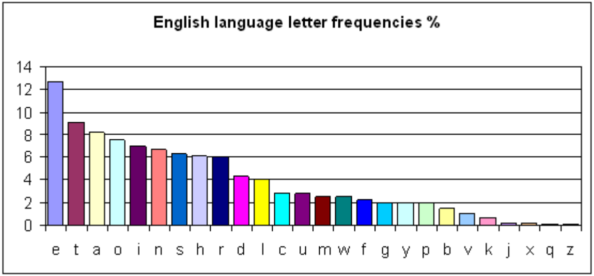
Turing's work in encryption

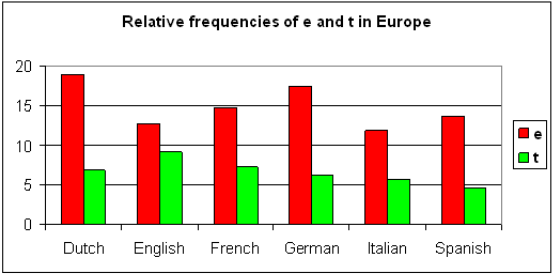
- 1937 Thinks about methods of encryption while at Princeton
- 1939 Joins Government Codes and Cypher School
- 1939 Meets Polish cryptologists in Paris
- 1939-1941 Breaks and rebreaks naval Enigma at Bletchley Park (Hut 8)
- 1942 Works on (mechanised) statistical attacks on Enigma
- 1942 Develops statistical attacks on Tunny (Lorenz machine)
- 1943-1945 Works on speech encryption (Delilah)
- 1945-1952 Continues to consult with GCHQ

Secure communication



Language statistics





Attacking a substitution cipher

Suppose that Alice and Bob are communicating using a substitution cipher. You wish to decrypt the following message which you intercept:

QX FPF JZB RPB BRX BXVKRXWT QPJX TBZWX.

You know the plaintext is in English, in which letter frequencies in decreasing order are:

E, T, A, O, I, N, S, H, R, ...

and you have a crossword solver's dictionary, of the sort that tells you all words of the form 'f ? ? t'. E.g. www.onelook.com.

Two Theorems in Probability

Bayes' Theorem

$$\mathbb{P}(A \mid B) \quad = \quad \frac{\mathbb{P}(B \mid A) \times \mathbb{P}(A)}{\mathbb{P}(B)}$$

the probability of A being true, given that B is true equals the probability of B begin true given that A is true $\times$ the ratio of A's probability to B's.

The Total Probability Theorem

If B_1 and B_2 are mutually exclusive events, one of which must occur (i.e. exhaustive) then

$$\mathbb{P}(A) \quad = \quad \mathbb{P}(A \mid B_1) \times \mathbb{P}(B_1) + \mathbb{P}(A \mid B_2) \times \mathbb{P}(B_2)$$

the probability that A is true is equal to the sum of probabilities of A being true given B_i is weighted by the respective B_i probabilities.

Statistical cryptanalysis I

The ciphertext we received:

QX FPF JZB RPB BRX BXVKRXWT QPJX TBZWX.
number of letters = 13, number of X's=6, number of B's=5

Is the plaintext in French?

Bayes' Theorem says

$$\begin{aligned}\mathbb{P}(\text{French} \mid \text{find E}) &= \frac{\mathbb{P}(\text{find E} \mid \text{French}) \times \mathbb{P}(\text{French})}{\mathbb{P}(\text{find E})} \\ &= \frac{0.147 \times 1/6}{6/13} = 0.053 \qquad (\text{about } 5\%)\end{aligned}$$

Statistical cryptanalysis II

The ciphertext we received:

QX FPF JZB RPB BRX BXVKRXWT QPJX TBZWX.
number of letters = 13, number of X's=6, number of B's=5

What is the probability of X=E, given that we know the plaintext is a major European language?

Total probability theorem:

$$\mathbb{P}(\text{X=E}) = \mathbb{P}(\text{X=E} \mid \text{Dutch}) \times \mathbb{P}(\text{Dutch}) + \ldots$$

Assumes the list of languages Dutch, English,... is exhaustive, so our probability calculation may only be accurate to a first approximation (but probably our values of $\mathbb{P}$(Dutch), $\mathbb{P}$(English), ... are estimates in any case).