The secrecy of a cipher is measured by:

**Definition:** The *key equivocation* $H_C(K)$ is the conditional entropy of $K$ given $C$:

$$H_C(K) = \sum_C p(C) \sum_K p_C(K) \log_2(1/p_C(K)).$$

If $H_C(K) \to 0$ as the length of $C$ increases, then the cipher is theoretically breakable, and the *unicity distance* is the shortest length $N$ of $C$ for which $H_C(K)$ is near 0, say $H_C(K) < 1$.

A cipher is *unconditionally secure* if $H_C(K) \not\to 0$ as the length $N$ of $C$ increases without bound.

**Example.** A one-time pad is unconditionally secure.
For most ciphers we can only approximate the unicity distance. We now derive a useful approximation to it.

Recall: $r = H(X)/N$, $R = \log_2 a$ and $D = R - r$.

Recall: There are $2^{rN} = 26^N$ $N$-letter messages, $2^rN$ of them are meaningful and $2^{rN} - 2^rN$ are meaningless.

Assume: All $2^rN$ meaningful messages have equal probability $2^{-rN}$ and all meaningless messages have probability 0.

Note that we are assuming the equally-likely case, which maximizes entropy and is the worst case.

Assume: There are $2^{H(K)}$ keys, and they are equally likely. That is, $p(K) = 2^{-H(K)}$ for each key $K$. 
A random cipher is one in which for each key \( K \) and ciphertext \( C \), the decipherment \( D_K(C) \) is an independent random variable uniformly distributed over all \( 2^{RN} \) messages, both meaningful and meaningless. This means that for a given \( K \) and \( C \), \( D_K(C) \) is as likely to produce one plaintext message as any other. Actually the decipherments are not completely independent because a given key must uniquely decipher a given message, so that \( D_K(C) \neq D_K(C') \) for \( C \neq C' \).

Assume we have a random cipher and suppose \( C = E_K(M) \). A spurious key decipherment or false solution of \( C \) is either \( C = E_{K'}(M) \) or \( C = E_{K''}(M') \) where \( M' \) is meaningful. (We are not concerned with meaningless false solutions as they are easily detected.) In the first case \( (C = E_{K'}(M)) \), the key \( K' \) may or may not decipher other \( C \) enciphered with \( K \).
For every correct decipherment there are $2^{H(K)} - 1$ other keys, each with probability

$$q = 2^rN / 2^{RN} = 2^{-DN}$$

of giving a false solution. Let $F$ be the number of false solutions. Then

$$F = (2^{H(K)} - 1)q \approx 2^{H(K) - DN}.$$

When $N$ is large enough so that $F < 1$, we have enough ciphertext to break the cipher. At the borderline case where $F = 1$, we have $H(K) = DN$. Thus $N = H(K)/D$ is approximately the unicity distance.

**Example.** DES is a block cipher with 56-bit keys and 64-bit blocks of plain and cipher text. 64 bits is 8 characters. For English, $D = 3.7$, so $N = H(K)/D = 56/3.7 = 15.1$ characters or about two blocks.