What is Good Encryption?

The following are suggested as tests of worth for current cryptographic practice:

- is based on sound mathematics;
- has been analyzed by competent experts and found to be sound;
- has stood the test of time.
An encryption algorithm is called *breakable* if, given enough time and data, an analyst can recover the plaintext.

*Most encryption algorithms are breakable* since the analyst can try all keys systematically. Being breakable doesn’t mean that it’s feasible to break.

The analyst must be able to recognize success. For that reason, having plaintext/ciphertext pairs available is often required.
A cryptosystem is *strong* if there is no analytic approach that is substantially faster than brute force—i.e., trying all of the keys one by one. *Most strong algorithms are still breakable.*

The larger the *keyspace*, the longer to find the key by search. How do you compute the size of the keyspace?

Many ciphers use a $n$-bit string as key. Given a small number of plaintext/ciphertext pairs encrypted under key $K$, $K$ can be recovered by exhaustive search in an expected time on the order of $2^{n-1}$ operations. *Why?*
The simplest building blocks of encryption are:

**substitution**: in which each symbol is exchanged for another (not necessarily uniformly), and

**transposition**: in which the order of symbols is rearranged.

It might seem that these are too naive to be effective. *But almost all modern commercial symmetric ciphers use some combination of substitution and transposition for encryption.*
Two things an encryption step can provide are:

**Confusion:** transforming information in plaintext so that an interceptor cannot readily extract it.

**Diffusion:** spreading the information from a region of plaintext widely over the ciphertext.

Substitution tends to be good at confusion; transposition tends to be good at diffusion.
Lessons

- An encryption algorithm is *breakable* if a systematic process will permit extracting the message.
- It is *strong* if there is not better attack that brute force.
- Most symmetric encryption algorithms use some combination of substitution and transposition to accomplish both confusion and diffusion.

**Next lecture:** Substitution Ciphers