Modern cryptography

- Agents (machines) handle communication and much of this communication is electronic.
- Classic problems of eavesdropping, disruption and corruption still exist.
- The implementation of these attacks is now by machine and can be automated - the attacks happen at machine speed.

Authentication

- For the most part machines need to know who they are communicating with.
- This is true even on secure networks.
- Cryptography can help with the issue of authentication and trust between agents.
- Is it possible to arrange for trust even without knowing who you are talking with? Yes! and cryptography can help with that too.

Error correction

- How can you tell if the data communicated has been corrupted?
- This is a problem whether the data has been encrypted or not although it becomes acute when the data has been encrypted.
- It is important to keep in mind data corruption when designing a cyptographic system - the system needs to be robust enough to handle the types of errors that are likely to occur.
- Sometimes you don’t want error correction!

Summary

It is important when designing crypto-systems to know

- what the problems are that you are trying to solve - military security, bank security, privacy of your phone, data corruption for video games
- what the threats are - hackers, blackmailers, eavesdropping, nuisances
- what the time frame is for the application - minutes or forever (or anything in between)
- what tools or technologies you have access to - fast computers, specialty hardware or the custodian

Vigenère's cipher, section 2.3

- Code the alphabet using 0 - 25: A - 0, B - 1, C - 2, ...
- We work with arithmetic modulo 26.
- This cipher encrypts strings of letters - we skip blanks. E.g.

  D O G
  3 14 6

- The cipher uses a code length k and a vector of length k of numbers mod 26.
- For example, if $k = 3$ and $v = (4, 7, 12)$ we encrypt DOG as follows:

$$(3, 14, 6) + (4, 7, 12) = (7, 21, 18)$$

  and that is the string HWT.

Vigenère's cipher, cont'd

- For longer strings we just code the first k letters as above and then start again with the next k letters until we finish the string.
- The sense of security comes from not knowing k as well as not knowing v.
- As we will see, this cipher is susceptible to a letter frequency attack.

English letter frequency

Letter frequency in texts, Beker-Piper, '82

a	b	c	d	e	f	g	h	i
.082	.015	.028	.043	.127	.022	.020	.061	.070
j	k	l	m	n	o	p	q	r
.002	.008	.040	.024	.067	.075	.019	.001	.060
s	t	u	v	w	x	y	z	
.063	.091	.028	.010	.023	.001	.020	.001	