Uses of Cryptography

- What can we use cryptography for?
- Lots of things
  - Secrecy
  - Authentication
  - Prevention of alteration

Cryptography and Secrecy

- Pretty obvious
- Only those knowing the proper keys can decrypt the message
  - Thus preserving secrecy
- Used cleverly, it can provide other forms of secrecy

Cryptography and Authentication

- How can I prove to you that I created a piece of data?
- What if I give you the data in encrypted form?
  - Using a key only you and I know
- Then only you or I could have created it
  - Unless one of us told someone else the key . . .

Using Cryptography for Authentication

- If both parties cooperative, standard cryptography can authenticate
  - Problems with non-repudiation, though
- What if three parties want to share a key?
  - No longer certain who created anything
  - Public key cryptography can solve this problem
- What if I want to prove authenticity without secrecy?

Cryptography and Non-Alterability

- Changing one bit of an encrypted message completely garbles it
  - For many forms of cryptography
- If a checksum is part of encrypted data, that's detectable
- If you don't need secrecy, can get the same effect
  - By encrypting only the checksum

Symmetric and Asymmetric Cryptosystems

- Symmetric - the encrypter and decrypter share a secret key
  - Used for both encrypting and decrypting
- Asymmetric – encrypter has different key than decrypter

Description of Symmetric Systems

- $C = E(K,P)$
- $P = D(K,C)$
- *E()* and *D()* are not necessarily the same operations

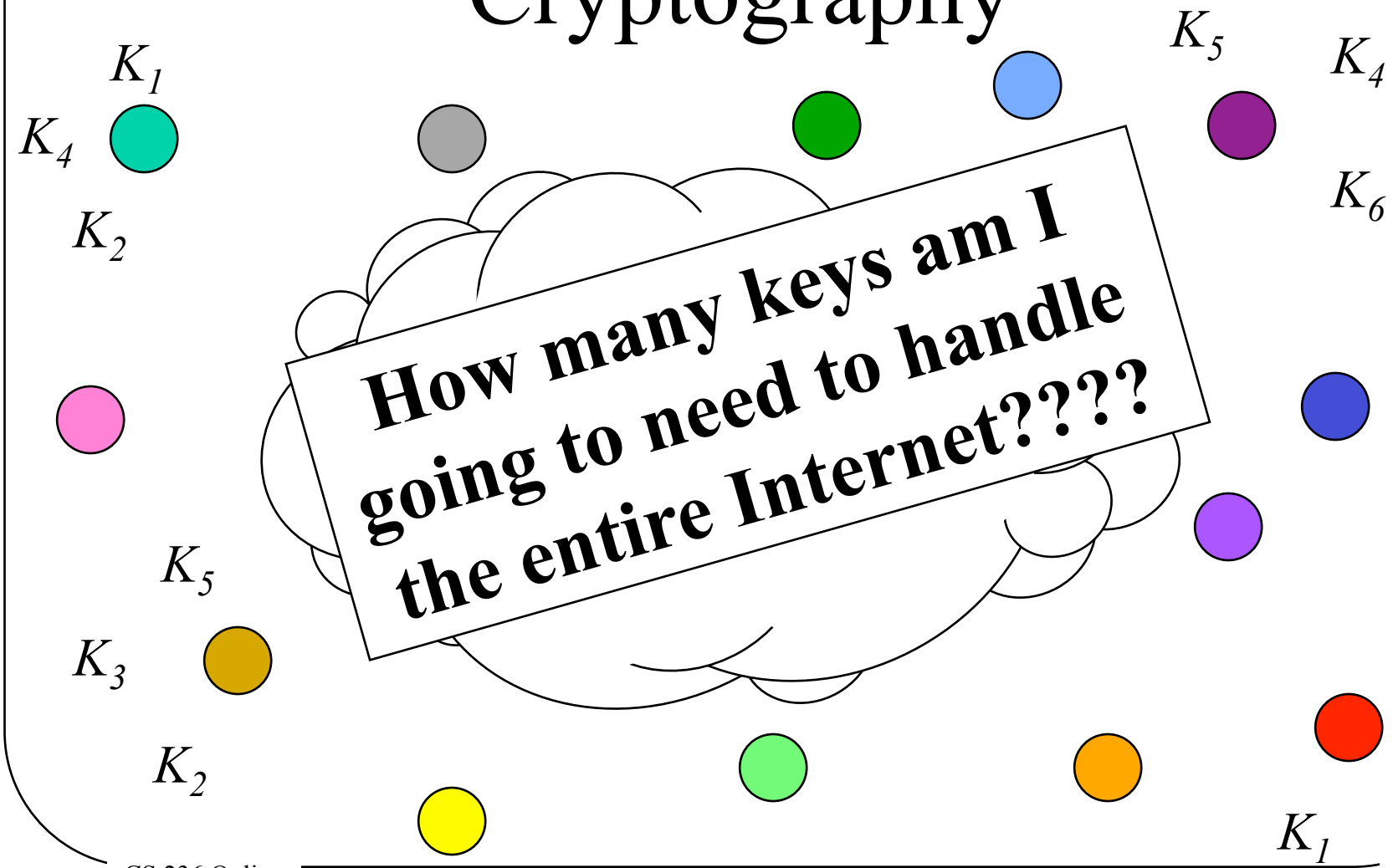
Advantages of Symmetric Key Systems

+ Encryption and authentication performed in a single operation
+ Well-known (and trusted) ones perform faster than asymmetric key systems
+ Doesn't require any centralized authority
  - Though key servers help a lot

Disadvantage of Symmetric Key Systems

- Encryption and authentication performed in a single operation
  - Makes signature more difficult
- Non-repudiation hard without servers
- Key distribution can be a problem
- Scaling

Scaling Problems of Symmetric Cryptography



Sample Symmetric Key Ciphers

- The Data Encryption Standard
- The Advanced Encryption Standard
- There are many others

The Data Encryption Standard

- Well known symmetric cipher
- Developed in 1977, still much used
  - Shouldn't be, for anything serious
- Block encryption, using substitutions, permutations, table lookups
  - With multiple *rounds*
  - Each round is repeated application of operations
- Only serious problem based on short key

The Advanced Encryption Standard

- A relatively new cryptographic algorithm
- Intended to be the replacement for DES
- Chosen by NIST
  - Through an open competition
- Chosen cipher was originally called Rijndael
  - Developed by Dutch researchers
  - Uses combination of permutation and substitution

Increased Popularity of AES

- Gradually replacing DES
  - As was intended
- Various RFCs describe using AES in IPsec
- FreeS/WAN IPsec (for Linux) includes AES
- Some commercial VPNs use AES
- Used in modern Windows systems
  - Also recent versions of Mac OS

Is AES Secure?

- No complete breaks discovered so far
- But some disturbing problems
  - Attacks that work on versions of AES using fewer rounds
  - Attacks that get keys quicker than brute force
    - But not practical time (e.g. in 2^{126} operations)
- But unusable crypto flaws often lead to usable ones
- Attacks on crypto only get better over time, never worse