1) Quizzes back on Wednesday!
2) Next part of course: Modern Cryptography (with Computers)
   a) Symmetric/Private Key
   b) Public Key

Private key - you and msg recipient share a private key that no one else has.

Most private key (modern) schemes are block ciphers - Plaintext is separated into chunks of n bits (0/1s), so n is what we call the block size.

Plaintext: 10110000 01001101 00111111 11011001

To manipulate bits in the computer, it's really helpful to know about bitwise operators.

Most important for crypto: XOR \( \oplus \) operator in code
### XOR

| b | \text{bitwise XOR} | a = 1001 0011 | b = 0101 1001 | \hline
| 1 | \hline
| b | \text{bitwise XOR} | a = 1001 0011 | b = 0101 1001 | \hline
| \text{bitwise OR} | a = 1001 0011 | b = 0101 1001 | \hline

128 + 16 + 3 = 147
64 + 16 + 9 = 89

(exclusive or means exactly 1 of the 2 items is true)

XOR "flips" the bits where there is a 1.

\[ \land a = 1001 0011 \]
\[ a = 1001 0011 \]
\[ a = 1001 0011 \]
\[ \land a = 0 \]

Inverse operation of "XOR by a" is "XOR by \( \bar{a} \)"

\[ a = 1001 0011 \]
\[ b = 0101 1001 \]
\[ \land \bar{a} = 1001 0011 \]
\[ 1101 1011 \]

\[ a >> 4 \]
\[ a \ll 4 \]

\[ a \gg 4 \]
\[ a \ll 4 \]

Common use

\[ a >> 4 \]

Right bit shift

\[ a \ll 4 \]

Left bit shift

1001 0011 \Rightarrow 1001

Chop off

1001 0011 0000
1) taking several ints, breaking them up byte by byte and XORing each byte

\[
\begin{array}{cccc}
& 8b.15 & 8b.15 & 8b.15 & 8b.15 \\
\end{array}
\]

a) extract 8 least significant bits

\[(1 \ll 8) - 1\]

\[
\begin{array}{cccc}
& 100000000 & - 1 & \rightarrow \\
\end{array}
\]

b) bitwise AND with this

\[
\begin{array}{cccc}
& 0000 & 0000 & 0000 & 1111 \\
\end{array}
\]

& mask 0000 0000 0000 11111111

\[
\begin{array}{cccc}
0 & 0 & 0 & 0 \times \\
\end{array}
\]