Introduction to Digital Logic

- Binary
- Hexadecimal

Doug Shook

Review Questions

- Convert the following decimal values into binary and hex:
- 260
- 131
- 314,159
- 2,147,483,647

Review Questions

- Convert the following binary values into decimal and hex:
- 011101
- 100111011011
- 0110000101
- 110001101000

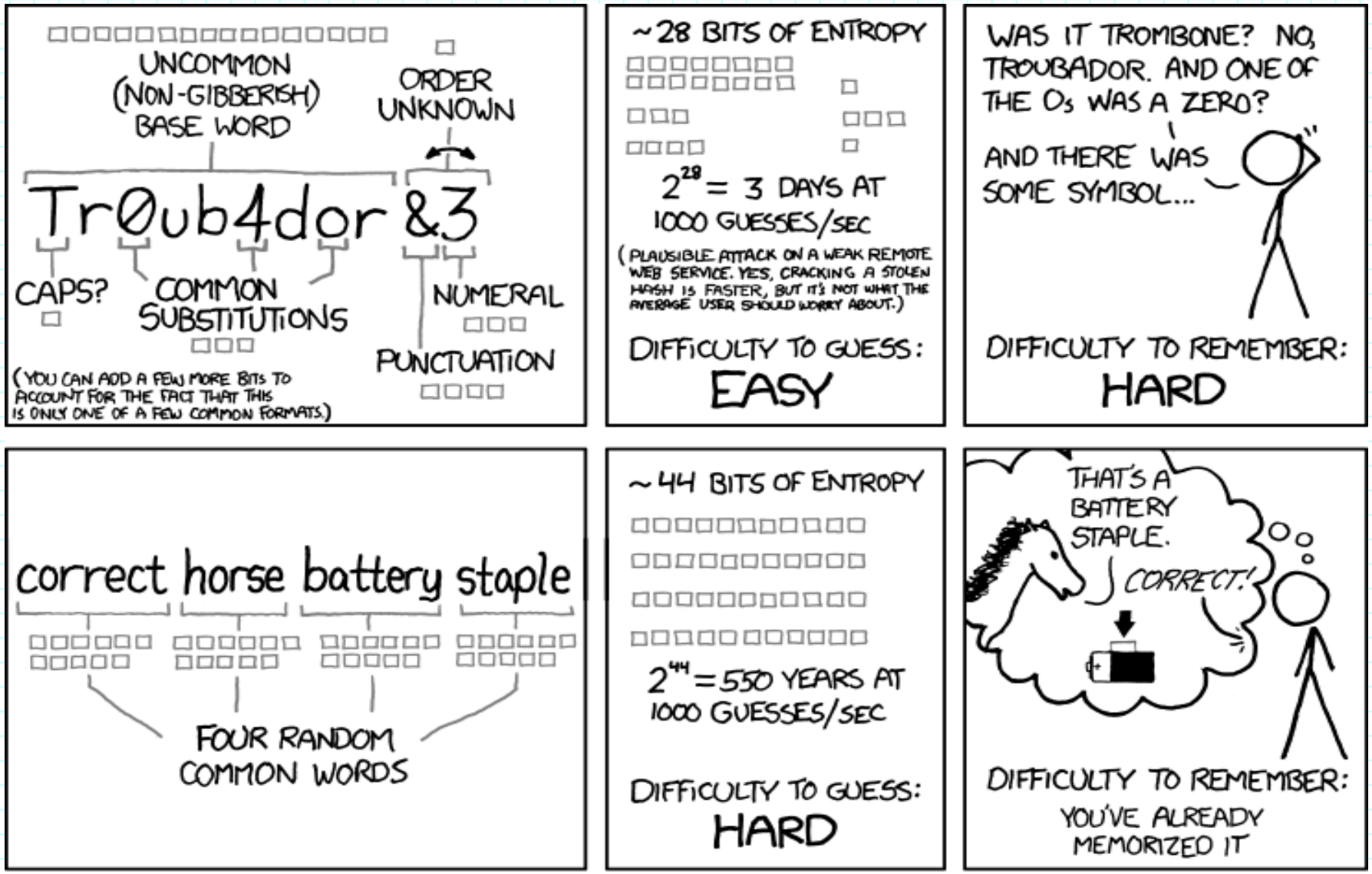
Review Questions

- Convert the following hex values into decimal and binary:
- 42
- 104A
- CAFE
- DEADBEEF

Review Questions

- State how many bits would be required to represent the following:
- 8 letter passwords that use only lower case
- 8 letter passwords that use lower and upper case
- 8 letter passwords that use lower case, upper case, and digits
- 8 letter passwords that use lowere case, upper case, digits, and 10 special characters.
- 24 letter passwords that use only lowercase

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Hexadecimal - Demo