CS Concepts

- Caesar cipher
- Vigenere cipher
- One-time pad
- public-key encryption
- one-way computation
- digital signature
- RFID
- WEP, WPA, PGP, RSA
- back door

Social Issues

- legislating back doors
- untappable communications
- internet commerce
- consumer apathy about communication privacy

Simple Encryption Scheme

- Caesar Cipher

GDKKN

- Shift each letter a fixed distance (right or left in the alphabet).

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Simple Encryption Scheme

- Caesar Cipher

WKH DQVZHU LV G

- Decode this encrypted message and you will know which answer to pick.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Better Encryption Scheme

- Substitution Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZWKBJLSIHCFGRAXEMNTUQPDOVY
```

- 26! or about $4x10^{26}$ different encoding/keys
- Caesar had just 26 – could just try them all

Decode This

- Key

  ABCDEFGHIJKLMNOPQRSTUVWXYZ

  ZWKBJLSIHCFGRAXEMNTUQPDOVY

JXQVTSPM

A. Synonym for laptop
B. Synonym for school
C. Synonym for house
D. Synonym for pencil
E. Synonym for table

Frequency Analysis

- Substitution Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZWKBJLSIHCFGRAXEMNTUQPDOVY
```

- 26! or about $4x10^{26}$ different encoding/keys
- Caesar had just 26 – could just try them all

Frequency Analysis

- Can you crack this one?

TSB YRNPBM GO JMIBRK IN ZFAPIRL IR TSB PIRK

Frequency Analysis

- Can you crack this one?

TS**B** Y**R**NP**B**M GO JM**IBR**K **I**N ZFAP**IR**L **IR** TS**B** P**IR**K

- R – 5, I – 5, B – 4
- E, T, A, O, I, N (most frequent)

Vigenère Cipher

- Cycle through a set of Caesar ciphers to combat frequency analysis.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM
DEFGHIJKLMNOPQRSTUVWXYZABC
```

. . .

- Key is the left column, which can be used to reconstruct the table.

Vigenère Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM
DEFGHIJKLMNOPQRSTUVWXYZABC
HIJKLMNOPQRSTUVWXYZABCDEFG
```

- How many letters must be transmitted to transmit the "key" to this Vigenère cipher?

A. 3

B. 4

C. 26 X 3 = 78

D. 26 X 4 = 104

Vigenère Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM
DEFGHIJKLMNOPQRSTUVWXYZABC
HIJKLMNOPQRSTUVWXYZABCDEFG
```

- Decode this: "ODUNQH"

A. BANDED

B. BANANA

C. BANGLE

D. BANTER

One-time Pad

- If the Vigenère key is as long as the text then it is called a one-time pad.
- Unbreakable in theory.

Vigenère Cipher

- "The amount of computation required to break a cipher by exhaustive search grows exponentially in the size of the key. Increasing the key length by one bit doubles the amount of work required to break the cipher, but only slightly increases the work required to encrypt and decrypt."
  - BTB pg. 173

Lessons of the Internet Age

- Breakthroughs happen but news travels slowly (Mary Queen of Scots)
  - Al-Kindi described how to decipher using frequency analysis over 9 centuries earlier.

Lessons of the Internet Age

- Confidence is good, certainty would be better.
  - "The Fundamental Tenet of Cryptography: If lots of smart people have failed to solve a problem, then it probably won't be solved (soon)."

Lessons of the Internet Age

- Having a good system doesn't mean people will use it.
  - "Hackers were able to steal more than 45 million credit and debit card records from TJX, the parent company of several major retail store chains, because the company was still using WEP encryption as late as 2005"

Lessons of the Internet Age

- The enemy knows your system.
  - Security through obscurity is no security.

Public Key Cryptography

- Pre-public key, assume the message will be intercepted so make it unreadable.
- Required the two parties to have a shared key.
- Breakthrough allows parties to create a key using a non-private communication, without ever meeting.

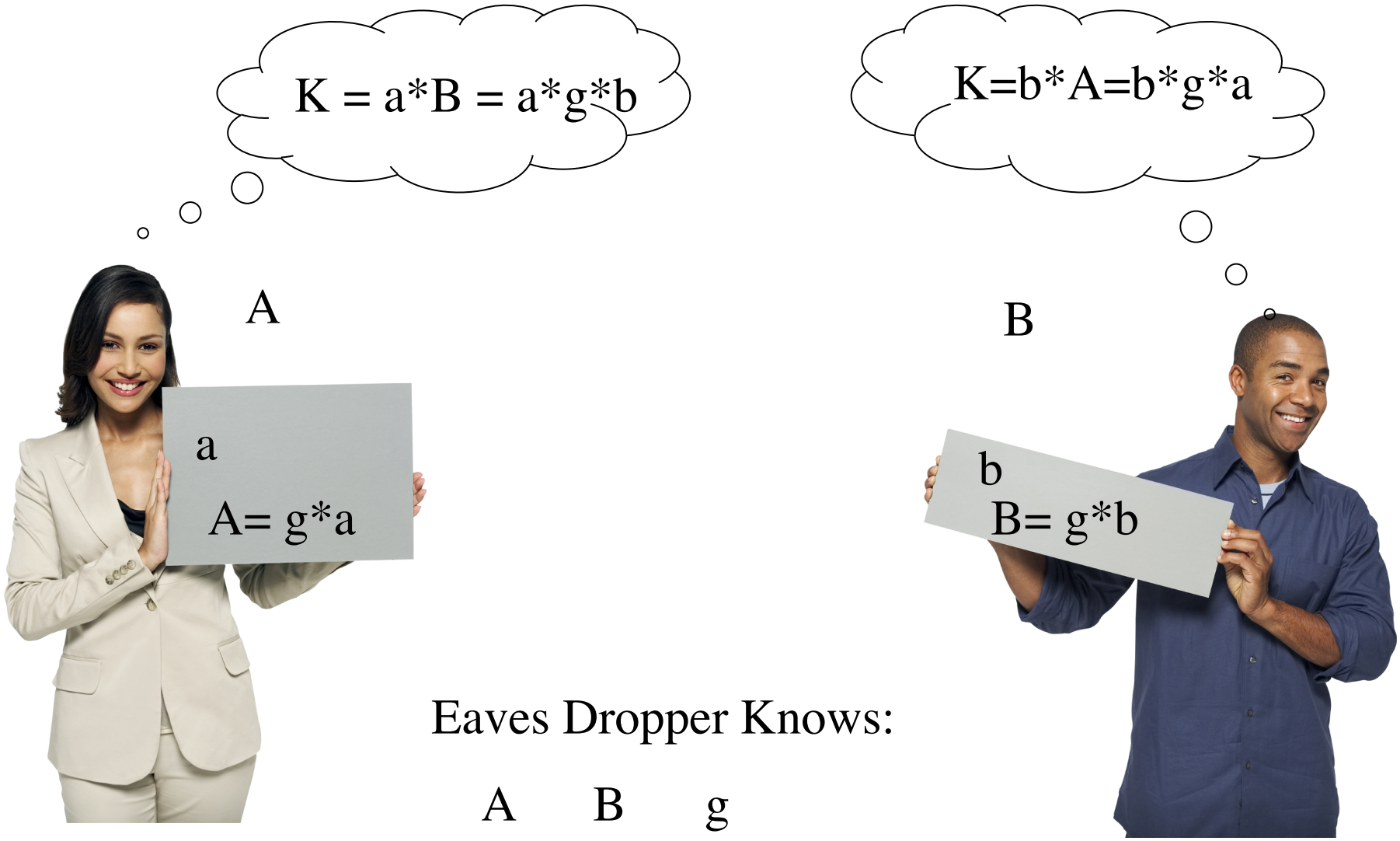
Diffie and Hellman

- didn’t need to have a shared secret (the key) in advance to communicate securely
- uses one-way computation and
- a key agreement protocol

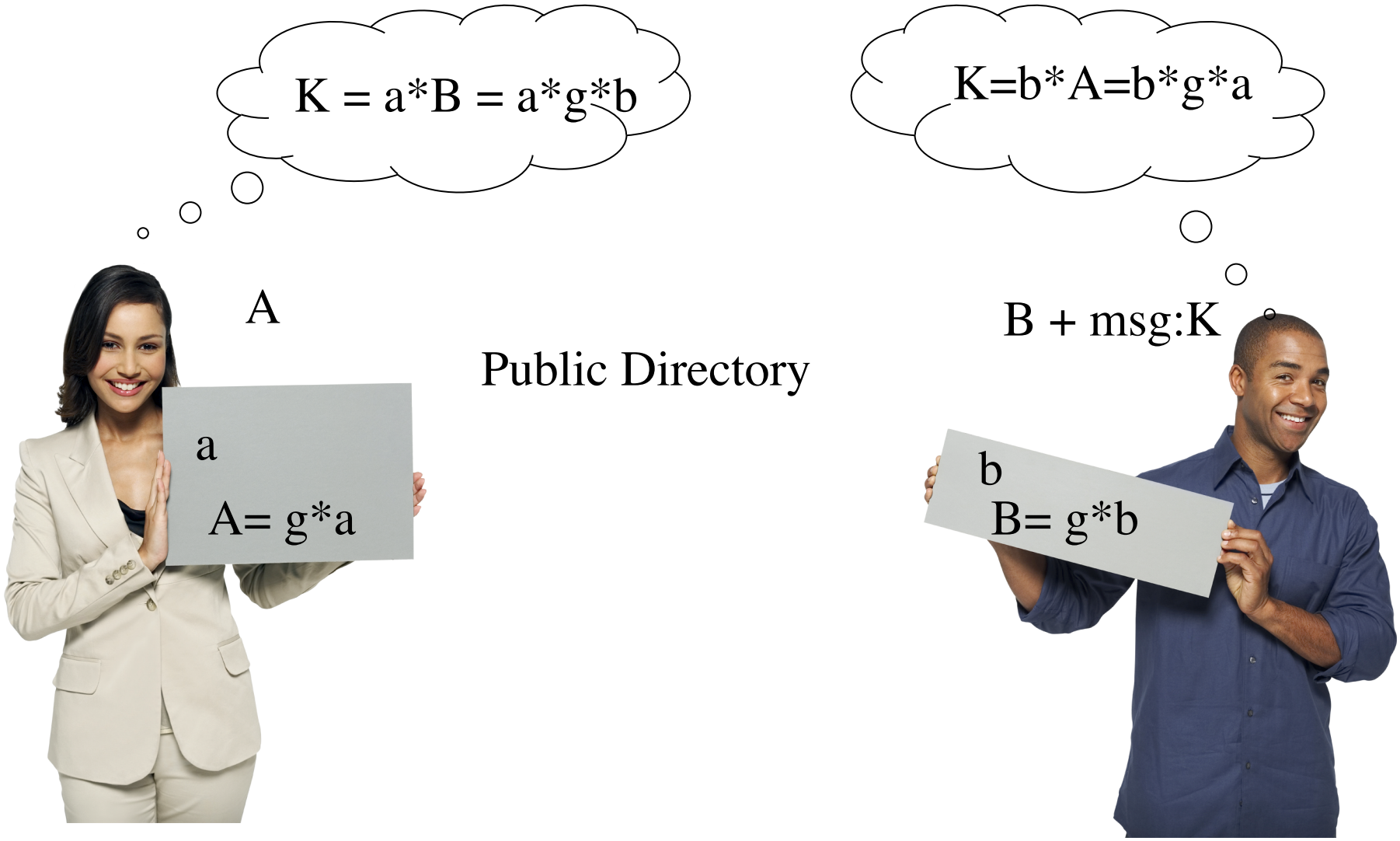
Key Agreement Protocol

- X*Y is easy but finding X given Y is HARD (not * is NOT multiplication)
- X*Y*Z = X*Z*Y
- everybody knows how to do X*Y and everybody knows some number g

Key Agreement Protocol



Public Key Messaging



Public Key Cryptography

- https://www.youtube.com/watch?v=YEBfamv-_do

A Shared Secret?

A. Using Public Key cryptography, one of the two communicating parties must first SECRETLY communicate a special “key” to the other that they then use to carry on the rest of their secret communication.

B. Using Public Key cryptography, ALL messages passed between the two parties can be read by a third party without risk of the secret communication being compromised.

Digital Signatures

- Send plain text message along with essentially an encrypted copy of the message as the “signature”.
- System relies on the fact that it is easy to encrypt a message with a private key (e.g. Alice’s a) and easy to decrypt a message with a public key (e.g. Alice’s A).
- Bob decrypts the “signature” with A and if he doesn’t get the original message back, then it was tampered with in some way.

RSA – Rivest, Shamir, and Adleman

- Found a way to compute private-public key pairs (e.g. a and A) such that they perform inverse operations.
- RSA(msg,a) = secret
- RSA(secret,A) = msg

RSA Encryption

- https://www.youtube.com/watch?v=wXB-V_Keiu8

Is that REALLY Alice's public key?

- How do you know you are really talking to Alice, or that was her key you found in that public directory?
- Enter certificates and certificate authorities.

Public Policy

- Escrowed Encryption Standard - Clipper Chip (Clinton 1994)
- Crypto Wars of the 1990s – civil liberties vs law enforcement
- Phil Zimmerman – (paraphrasing testtimony to Congress) before the internet surviellance was hard, like fishing with a hook and line, now it is easy, like fising with a net
- PGP – Pretty Good Privacy – encryption company

CS Concepts

- Caesar cipher
- Vigenere cipher
- One-time pad
- public-key encryption
- one-way computation
- digital signature
- RFID
- WEP, WPA, PGP, RSA
- back door

Social Issues

- legislating back doors
- untappable communications
- internet commerce
- consumer apathy about communication privacy