

A night cityscape, likely New York City, with numerous skyscrapers illuminated. Overlaid on the image is a network diagram consisting of white dots connected by thin white lines, forming a web-like structure across the sky. A solid red vertical bar is positioned on the far left edge of the image.

# CableLabs<sup>®</sup>

## Artificial Intelligence and the Global Economy

# AI=MACHINE LEARNING

1. Machine Learning => massive amounts of data

Cloud and mobility means applications and data can be accessed from anywhere.

Extraordinary advances for multinational enterprises:

Supply chain planning, targeted marketing, consumer preferences, gig economy, etc.

# THE GLOBAL ECONOMY

Enabled by the Internet -and Big Data-

Extraordinary advances for countries

Trade, growth, epidemiology, defense, research, financial markets,  
growth, etc.

# A WORLD WITHOUT BORDERS

CableLabs®



# INTERNET-THE DREAM

- Global access to information.
- Ability to share data for large studies.
- Machine learning for pattern recognition, globally.
- Learning from others!

And what about **Privacy**?



# TROUBLE IN PARADISE: VIRTUAL BARRIERS



© 2007. Her Majesty the Queen in Right of Canada, Natural Resources Canada. / Sa Majesté la Reine du chef du Canada, Ressources naturelles Canada.

# REAL TROUBLE

- Countries do not allow access to each other's data.
- Enterprises not having access to their own data if in different countries.
- Balkanization of information.
- Privacy is the driver behind virtual barriers.

# D°ES IT MATTER?

How do you aggregate information (hospitals, demographics, economic data?)

How do you find commonalities in data?

How do you conduct negotiations if prices cannot be revealed?



# Two Approaches

1. Institutional. Public policies. Hard to implement.
2. New protocols. Easier to design and deploy.

# SECURE MULTIPARTY COMPUTATION

Parts of the data belongs to multiple owners.

They collectively want to perform analytic studies on the entire dataset.

While respecting the privacy and security concerns of each individual party.

# Secure Multiparty Protocol



Alice's list:  $a, b$

Alice generates secret key  $x$

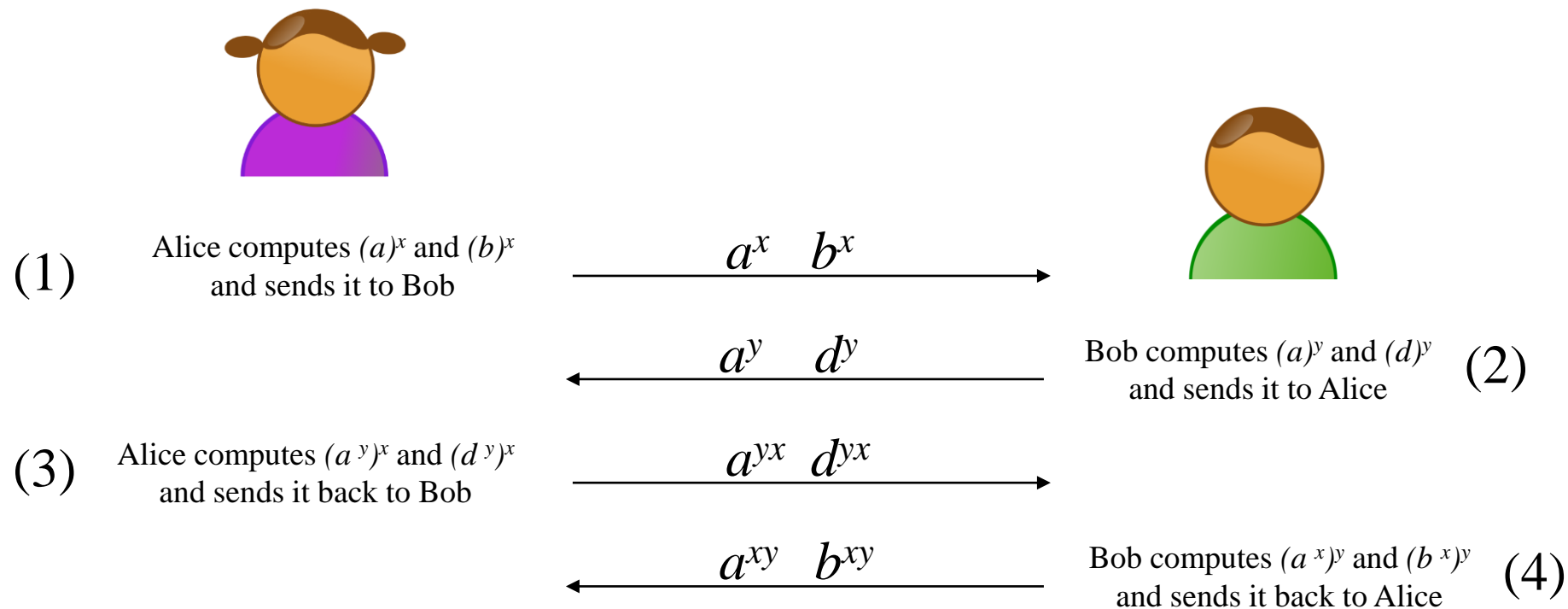


Bob's list:  $a, d$

Bob generates secret key  $y$

- $a, b, x, y$  are integers.
- Alice and Bob agree on a common prime number  $p$ .
- All computations are done modulo  $p$ .

# Secure Multiparty Protocol



Since  $a^{xy} = a^{yx}$  they know they both have  $a$   
but Bob doesn't know Alice has  $b$  and vice versa.

# How secure is it?

Based on the intractability of the discrete logarithm.

Given integers  $a$  and  $b$  and prime  $p$ , it is computationally hard to find integer  $x$  such that,

$$b^x = a \pmod{p}$$



# HOW TO PROTECT - AND ACCESS - DATA

CableLabs®

Biggest issue for the information economy.

Balkanization of data will continue.

New forms of computation will be needed.

Securing the data, not just the wires.

# Summary

AI and Cloud:

Enablers of a global economy that benefits all.

Security concerns led to the creation of virtual barriers.

Those barriers prevent us from leveraging that immense sea.

Solutions can be institutional or algorithmic (protocols).

We also need to secure the information (quantum networks)