Asymetric cryptography 101

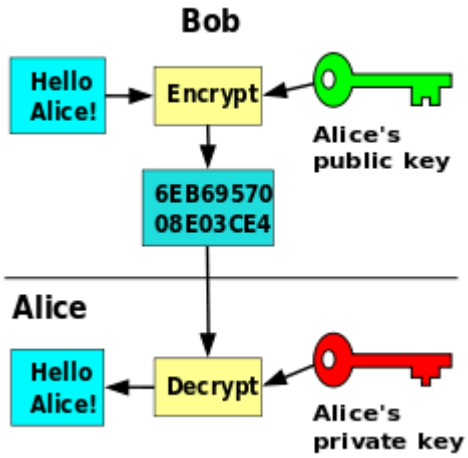
Fred Mora

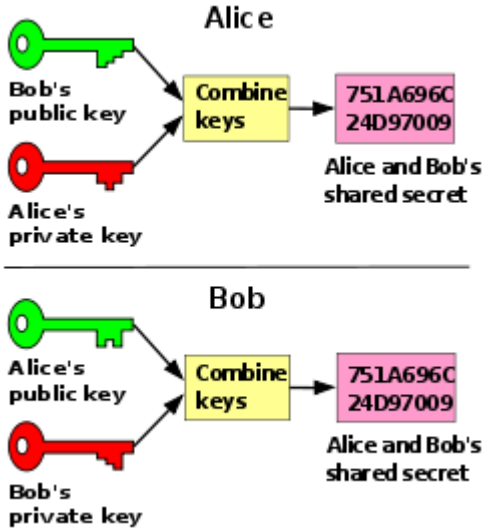
Secrets without swapping keys

- Encryption is now taken for granted
- We use it with HTTPS (Web), SSH, etc.
- We don't have to worry about secret keys. But that wasn't always the case.
- Up to the 80s, before users could exchange encrypted messages, they needed to agree on a secret key
  - It could be the offset of the rotors on a German Enigma machine
  - Or the one-time pad of a Soviet spy in New York
  - Or a secret DES key

Asymmetric crypto

- Modern crypo systems don't share a common key
- Each user creates a key pair:
  - a public, easily accessible key
  - a private, secret key.
- The public key can decrypt what the private key has encrypted, and vice versa
- Also, say Alice and Bob want to exchange messages
  - Each can use their private key and the other user's public key
  - They combine them to generate a shared secret key
  - They use this shared secret to swap messages.





And we can get fancy, too

- This opens interesting possibilities.
- Signing a message:
  - Alice computes the checksum C of her message M to Bob
  - She encrypts the checksum with her private key
  - She concatenates M and the encrypted checksum
  - She encrypts the whole thing with Bob's public key
  - She sends it to Bob
  - Bob decrypts the received data with his private key
  - He can read the message M
  - He decrypts the checksum with Alice's public key
  - He recomputes the checksum and verifies it matches.

The math behind it

First, some reminders

- Primes:
  - A prime number has no divider (except 1, but who cares)
- Modulo:
  - Noted “mod” or % operator in C
  - A mod B means the remainder of A/B
  - Example: 7 mod 5 is 2. So is 22 mod 5.
- Exponents:
  - (A^n)^m = A^(n*m)
  - Example: $(2^2)^3 = (4)^3 = 64$, $(2^3)^2 = (8)^2 = 64$

Trap-door functions

One-way computation!

Concept	Example
Take a prime number q and some numbers A and X less than q	q = 11, A = 3, X = 5
Compute $Y = A^X \bmod q$	$Y = 3^5 \bmod 11 = 243 \bmod 11 = 1$
If I just give you Y, A and q, can you figure out X?	$3^X \bmod 11 = 1$, what is X?

- Turns out it is a very hard problem.
- You need to try out possible solutions.
- Best algorithm needs sqrt(q) trials.
- Take a very large prime q and guessing becomes impossible

Fine, so how does that work?

- Alice and Bob want to exchange a message over the phone.
- They don't want Nancy the NSA spook to read it. They need a secret key.
- They pick A and q over the phone (so Nancy knows A and q)
- Alice and Bob each pick a secret X called X1 and X2
- Alice computes $Y1 = A^{X1} \bmod q$, Bob computes Y2
- They publish (or discuss over the phone) the value of their Y
- Nancy listens…
- Alice and Bob hang up. Time to compute the key.

Computing the key

Concept	Example: q = 11, A = 7, X1 = 2, X2 = 3
X1, X2 kept secret. Y1, Y2 public.	Alice: $Y1 = A^{X1} \bmod 11 = 5$ Bob: $Y2 = A^{X2} \bmod 11 = 2$
Each user takes their X and the Y from the other user.	Alice has X1 = 2 and Y2 = 2 Bob has X2 = 3 and Y1 = 5
They compute $K = Y^X \bmod q$	Alice: $K = Y2^{X1} \bmod 11 = 2^2 \bmod 11 = 4$
	Bob: $K = Y1^{X2} \bmod 11 = 5^3 \bmod 11 = 4$

Alice and Bob's computations produce the same key!

Alice:

$K = Y2^{X1} \bmod 11 = (A^{X2})^{X1} \bmod 11 = A^{X2.X1} \bmod 11$

Bob:

$K = Y1^{X2} \bmod 11 = (A^{X1})^{X2} \bmod 11 = A^{X1.X2} \bmod 11$

Using the key

- Using the common key, Alice and Bob can now encrypt, exchange and decrypt messages
- Yet they never sent the key to each other.
- For each user, X is the private key, Y is the public key.
- In practice, the selected integers are very large (e.g., 1024 or 2048 bits)

Encryption and decryption

- Older cryptography used a symmetrical, reversible encryption
  - Algorithm S encrypts and decrypts.
  - Better keep S secret
- Modern cryptography systems use well-known pair of functions (or algorithms) noted E for encryption and D for decryption.
  - E and D are common knowledge, but the encryption relies on keys.
  - E and D paired with private key X and public key Y
  - E_X (encryption with X) and D_Y (decryption with Y) are inverse of each other, and vice versa: For a key K and a message m,
    $D_X(E_Y(m)) = m$ – Encrypt with public key, decrypt with private key
    $D_Y(E_X(m)) = m$ – Encrypt with private key, decrypt with public key

Example: SSH

- Generate a key pair (here, using the RSA algo):

```
$ ssh-keygen -t rsa
# generate id_rsa and id_rsa.pub in your ~/.ssh dir
$ ssh-copy-id remote.example.com
fred@ remote.example.com's password:
# Now we can SSH in without a password
$ ssh  remote.example.com
fred@remote:~ $
```

Is privacy a crime? Governments think so.

Manhattan DA: iPhone encryption helps terrorists (Press, April 2015)

'Tech giants who encrypt comms are unwittingly aiding terrorists', claims ex-Home Sec Blunkett

Labour MP is never far away from Fear Agenda script

(The Register, Nov. 2014)

FBI Director: Apple, Google encryption aiding criminals and terrorists (Press, July 2015)

Feds want backdoors in cyphers

- Statism vs. individualism
- Surveillance vs. privacy
- Governments (including US) trying to mandate backdoors in encryption
- This is a throwback to the 90s Clipper chip
  - Contained a "law enforcement key"
  - Rejected after protests
- Today, new attempts at forcing backdoors in encryptions
- Opponents are intimidated
- Usual arguments:
  - "Honest people won't care"
  - "But only law enforcement would have the key"
- Yeah, about that...
- How good are the Feds at keeping confidential info?

The Feds' unmatched confidentiality track record

- Long tradition of leaking the most important secrets
- Even in time of great danger:

Oops. A network of Soviet agent within the White House, you say? There go our secrets.

A long and ~~sordid~~ storied tradition

- 2013: US soldier Bradley Manning sentenced to 35 years in Wikileaks case
- 2014: Former CIA agent Edward Snowden leaks NSA top-secret info, flees to Moscow (Used flaws in NSA's MS Sharepoint servers)
- But the best is yet to come…


THE BALTIMORE SUN

baltimoresun.com

A new approach to regional produce

'CRUSH' IS BACK

A split verdict in leaks by Manning

Private is not guilty of aiding enemy, but still could get 136 years

Up to 300 in city got inflated tax break

Homeowners to pay more after errors in historic credit

The Washington Post

Man who leaked NSA secrets steps forward

A REPORTER'S ACCOUNT

To leaker, personal risks were clear

EDWARD SNOWDEN: 'I'M NOT GOING TO HIDE'

Booz Allen consultant could face prosecution

The OPM "hack"

- 2015: Office of Personnel Management (Fed's HR dept.) intrusion revealed
- "Hackers" had been copying files for months
- Problem found during a demo of an Intrusion Detection System
- Everything was live online
  - 25 million personal dossiers of every present and past Federal employee
  - FBI investigation files for every clearance holder (investigations includes family and friends)
  - > 1 M fingerprints of top-secret field agents!

But four people familiar with the investigation said the breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, which has a networks forensics platform called CyFIR. CyTech, trying to show OPM how its cybersecurity product worked, ran a diagnostics study on OPM's network and discovered malware was embedded on the network. Investigators believe the hackers had been in the network for a year or more. (WSJ, June 10, 2015)

A shining example of IT management

- 11 out of 47 "hacked" systems still using older Windows version.
- Contractors hired to manage some systems
- Contractor hired subcontractors…
- Including foreign nationals…
- … Working in Brazil and China

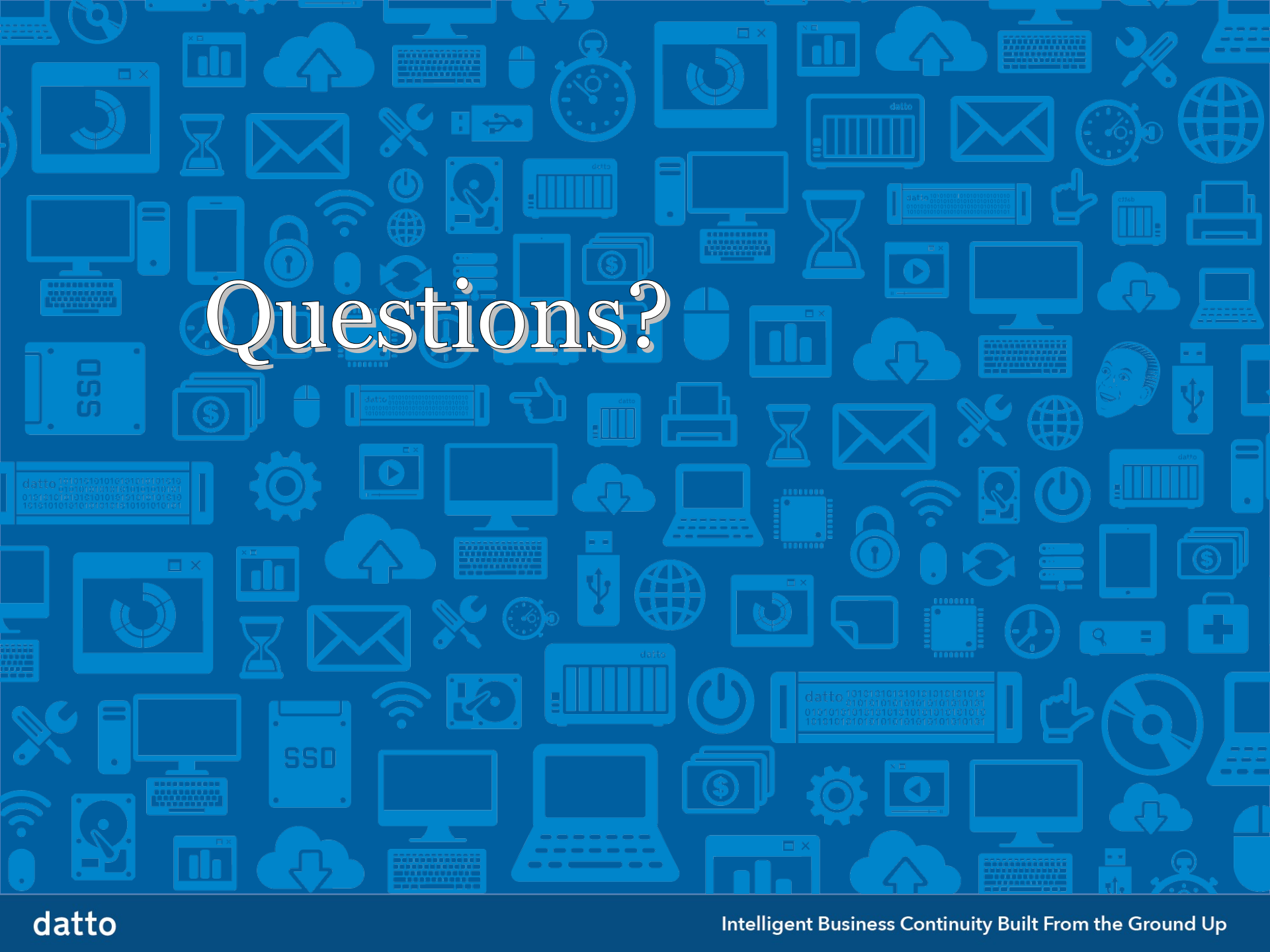
Some hackers

- But wait, there's more!
- "Encrypting personal files wouldn't have helped," says DHS.
- Oh, really, and why?
- Because the "hackers" used admin credentials from a subcontractor...
- ...who was a freelance Chinese national working from his home in Beijing.
- Must have been really hard to copy these files.

- The fingerprints are the most damaging
- Will let foreign services identify covert American operatives

So, is gummint backdoors a good idea?

- NO.
- If they were able to keep a secret...
  - Doesn't matter which party holds the executive, they shouldn't have that kind of power.
  - It's a matter of principles
- And since they provably aren't...
  - This is akin to a burglar that steals your files...
  - Then dumps copies in rest stop parking lots...
  - ...In several foreign countries.


Questions?