CRYPTOGRAPHY 099

DIFFIE-HELLMAN-MERKLE KEY EXCHANGE

WHO WHAT WHERE WHY HOW

@jeffrade

Why?

- We agree on a secret key.
- Then use this secret key to encrypt and decrypt our messages.
- But how do I tell you what the secret key is?
- This is known as the key distribution problem.

WHO?

- Whitfield Diffie
- Independent security expert & cryptographer
- Studied mathematics and graduated from MIT in 1965

WHO?

- Martin Hellman
- Professor at Stanford University
- Peers called him crazy for researching cryptography since NSA was doing the same (would be in competition).

Who?

- Ralph Merkle
- Also at Stanford University and worked with Hellman
- Hellman was his doctoral advisor

Where?

- Stanford University
- When Diffie and Hellman met, they instantly worked well together.
- Hellman couldn't afford to hire Diffie, so Diffie enrolled as a graduate student
- Diffie's wife was also in academia and her income helped Diffie stay independent to get to this point and continue on.

WHAT?

- Remember the key distribution problem (or key-exchange problem)?
- Can we solve this in the real world with physical boxes & locks?
- Yes!
- I put my message in a box, add my pad lock and send it to you (USPS).
- You receive it, add your pad lock and send it back to me.
- I receive it, remove my pad lock and send it to you.
- You receive it, remove your pad lock and read my message.

WHAT?

- Diffie used this idea as inspiration and needed a one-way mathematical function.
- Easy to do one-way, but difficult to do the other way (i.e. undo).
- Multiplication is a two-way function – just divide to undo.
- Multiplying two large primes is easy – but finding them is hard (one-way function).
- Another cryptic system relies on this fact.

WHAT?

- The focus came to modular arithmetic as a way to create their one-way function.
- In computer science, we know this as modulus or remainder function.
- Is the variable `i` even? Simply test if: `i % 2 == 0`
- We also learned modular arithmetic as kids. What time is 14 o'clock?
- Also known as clock arithmetic and a good visualization

WHAT?

- After years of research, Hellman devised a strategy to solve the key-exchange problem in 1976.
- It is quite elegant, fairly simple and regarded as one of the biggest breakthroughs in cryptography in the past few centuries.
- Computers and modern encryption has made cryptanalysts obsolete (i.e. breaking the cipher - Alan Turing and his work during WWII against enigma).
- Today, we safe-guard keys and strengthen encryption.
- Social hacking has become more popular – it is the least resistant.

HOW?

- Primer - Dre's Hackweek winner:
- E.g. `pool = [1,2,3,4,5,6,7,8,9,10,11,12]`
- E.g. `Ticket_hash = 2134` (i.e. really big number)
- `let volunteer = pool[ticket_hash % pool.length]`
- Pick any large number and `volunteer` will always be in range `[0 : 11]`

How?

- Back to Diffie-Hellman - Hellman came up with the following:
- Two parties agree on values `a` (generator) and `p` (large prime) and can be public.
- Each party picks a secret number (Bob picks `x`, Alice picks `y`) between 1 and `P-2`
- Bob computes `PK_B = a^x mod p` and Alice computes `PK_A = a^y mod p`
- Each party publicly sends their `PK_B` and `PK_A` (inside the clock, `< P`)
- Bob computes `PK_A^x mod p` and Alice `PK_B^y mod p` (key exchange complete!)
- Proof: `PK_A^x mod p = PK_B^y mod p = a^x^y mod p = a^y^x mod p = a^(x*y) mod p = a^(y*x) mod p` (equal by communitive property)

How?

- The prime number p has to be very large – 2048 bits ($100M can break 1024 bits – NSA, Amazon, Putin, etc.)
- Breaking the encryption is called "solving the discrete logarithm problem").
- Remember the number 'a' chosen as a generator for `a^x mod p`?
  a is usually a smaller prime number and it must produce a cyclic "table" when computing values `a^x mod p`.
- Basically, this "table" is a mathematical set that is between `0` and `P–1`
- Today Elliptic-curve Diffie–Hellman (ECDH) is used (faster and more secure against attacks).

NEXT?

- Diffie came up with the IDEA of public-key cryptography(asymmetric encryption)
- Encrypt a message with a public key and decrypt it with the private key
- Eventually a solution was invented in 1977 by a team of three at MIT: Adleman, Rivest and Shamir.
- Adleman was the mathematician on the paper and being humble, didn't want his name on it.
- But Rivest insisted so there was a compromise – Adleman's name would be listed last. So today, we don't know this system as ASR, but RSA.

Questions?

- The Code Book by Simon Singh (highly recommend)
- Elementary Number Theory and Its Applications by Kenneth H. Rosen