EECS 3481

APPLIED CRYPTOGRAPHY

SELECTED TOPICS

PROF H ROUMANI
Dept. of Electrical Engineering and Computer Science, York University

1

TOPICS

- **KEY DISTRIBUTION**
  Symmetric & Asymmetric Schemes (SKD & AKD)
- **KEY AGREEMENT**
  The Diffie-Hellman Exchange (NO-KD)
- **KEY STORAGE**
  Secret Splitting and Sharing
- **QUANTUM CRYPTOGRAPHY**
  SHOR'S ALGORITHM* & *BB84 (QKD)

2

2

SKD

SYMMETRIC KEY DISTRIBUTION

3

3

Regular SKD

Given n endpoints, i.e. applications running on hosts, we need to enable any pair to communicate securely via symmetric means (no public / private keys).

- Each endpoint needs n-1 secret keys
- Need couriers to deliver $n(n-1)/2 = O(n^2)$ keys!
- Must redo the delivery fiasco periodically*.

**Symmetric keys have a lifetime/lifecycle and an expiry date (length/ usage dependent), hence the periodic "key rollover".*

4

4

SKD via KDC

Given n endpoints, i.e. applications running on hosts, we need to enable any pair to communicate securely via symmetric means (no public / private keys).

- Designate one point as a *Key Distribution Centre.*
- Have each endpoint share one secret key with KDC
- This key is *not a session key*
- For sessions, *ephemeral* keys are JIT-generated
- O(n) courier deliveries (initially and periodically)

5

5

KDC Example

- A wants to communicate with B
- A creates a temporary session key K_S
- A → KDC: ID_A || ID_B || $E(K_A, K_S)$
- KDC creates a ticket $T=E(K_B, ID_A \,||\, K_S)$
- KDC → A: ID_B || T
- A → B: T
- A and B now share an ephemeral session key K_S

6

6

KDC Exercises

- Is KDC a BN (bottleneck) ?
  Comment on this in terms of scalability.
- Is KDC a SPOF (single point of failure) ?
  Comment on this in terms of availability.
- Is KDC a Vulnerability ?
  Comment on this in terms of security.

Can federated trust (a hierarchical scheme) mitigate some of the KDC risks pointed out above?

7

7

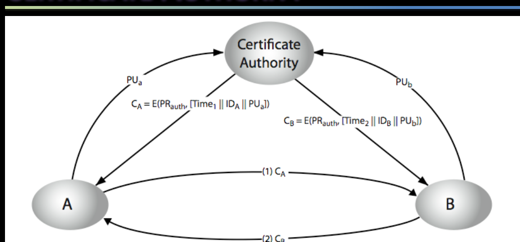
AKD

Asymmetric Key Distribution

8

8

Certificate Authority

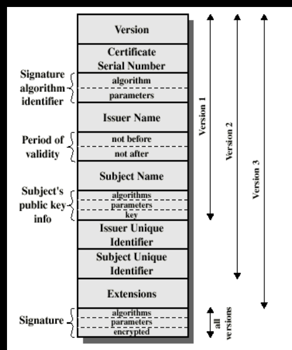


- A and B gets their public keys signed by the CA. Done once.
- To communicate they exchange their certificates.
- To scale, create a CA hierarchy to establish federated trust.

9

9

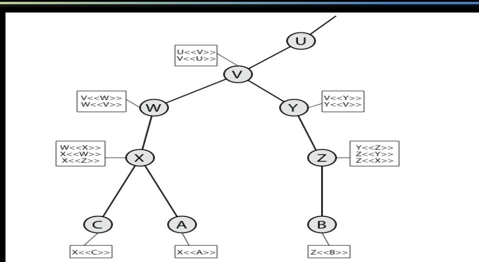
X.509 Certificate



10

10

Federated Trust



- S«E» means a certificate for E signed by S.
- When a new CA W is created, it holds W<<V> and V<<W>>
- A trusts B via the chain: X«W»W«V»V«Y»Y«Z»Z«B» => X«B»
- See https://ssl.netcraft.com

11

11

NO-KD

The Diffie-Hellman Key Exchange

12

12

Diffie-Hellman Key Exchange

Public: a large prime **p** *and a primitive root* **g**:

- Alice picks **aX** in [2,p-2] *(aX = her DH private)*
  She sends aY = g^{aX} (mod p) *(aY = her DH public)*
- Bob picks **bX** in [2,p-2] *(bX = his DH public)*
  He sends bY = g^{bX} (mod p) *(bY = his DH public)*
- Both compute the received raised to their private
  A shared session key K emerges => Key-Agreement
- Pick a subset of K's bits for DES, AES, OTP, or any other symmetric cipher.

No keys to lose or leak + Forward Secrecy.

13

13

Discrete Logs Math

Given a prime p and some base g in 2..p-1:

- X = g^x (mod p). **x** the *discrete log* of X in base g.
- The multiplicative subgroup generated by g has an order that divides p-1.
- If g is chosen as a *primitive root* of p then its subgroup's order will be p-1.
- See the posted spreadsheet to get a feel.

14

14

Man In The Middle Attack

- Beat a Chess Grandmaster!
  You can easily be the world second best !
- Person in the middle
  Eve injects herself in between Alice and Bob,
  She talks to Alice masquerading as Bob, and
  talks to Bob masquerading as Alice.

The attack exploits the lack of authentication (sender integrity) in the protocol. Hence, we should augment it with integrity countermeasures.

15

15

SS

KEY STORAGE
SECRET SPLITTING & SHARING

16

16

Secret Splitting

Split a secret M into W shares:

$s_1, s_2, \ldots s_W$

such that:

1. All shares have the same security strength.
2. All W shares are needed to reconstruct M.
3. If B=union of all but one share: $H(M|B) = H(M)$

H(E) is the entropy of event E. It is a measure of what we don't know about it. Its unit is bits.

17

17

Secret Splitting

Split a secret M into W shares $s_1, s_2, \ldots s_W$ such that:

1. All shares have the same security strength.
2. All W shares are needed to reconstruct the secret M
3. If B is the union of all but one share: $H(M|B) = H(M)$

Splitting Scheme:

- Choose a large-enough bit size n to accommodate all shares. All computations are done in n bits.
- Generate W-1 n-bit, distinct, non-zero random integers s_k
- Distribute the W-1 shares: $s_1, s_2, \ldots s_{W-1}$
- Distribute the share $s_W = XOR(s_k)$ xor M, k = 1 … W−1

To reconstruct, compute $XOR(s_k)$, k=1…W

18

18

Splitting Example

Split the secret M=90 to W=2 shares.
We choose n=8. Hence M = 01011010

Share #1
s1 = random = 235 = 11101011

Share #2
s2 = s1 xor M = 177 = 10110001

Combine
Find the secret
M = s1 xor s2

19

19

Secret Sharing

Split a secret M into W shares s_1, s_2, … s_W such that:

1. All shares have the same security strength.
2. Any T (T ≤ W) shares can reconstruct the secret M
3. Cannot reconstruct M with less than T shares.
4. If B is the union of fewer than T shares: H(M|B) = H(M)

Sharing Scheme (known as Shamir's threshold scheme):

- Choose a large-enough prime modulus p to accommodate all shares. All computations are done mod p.
- Generate T-1 distinct, positive random integers $s_i < p$
- Construct $y = f(x) = M + \sum s_k k^i$, k = 1 … T−1
- Generate W distinct x_k and deal the shares: (x_k , y_k=f(x_k))

To reconstruct, compute f(0)

20

20

Sharing Example

Threshold Scheme [3,4] with p = 19
W=4, T=3. Let the secret M be 12

Prep
s1 = 14, s2 = 3
$y = f(x) = 12 + 14x + 3x^2 \pmod{19}$

Deal
x1 = 1, x2 = 2, x3 = 3, x4 = 4
→ [1, 10], [2, 14], [3, 5], [4, 2]

Combine
Pick any three and plug in $f(x) = M + ax + bx^2$
Solve 3 equations in 3 unknowns → M

21

21

QKD

QUANTUM CRYPTOGRAPHY SHOR & BB84

22

22

THE CLASSICAL WORLD: THREE PILLARS

They inform our intuition. Our math formalizes them:

1. **Realism** *[Ontology vs Epistemology]*
   Properties exist even if we don't measure.
   The moon is there even if no one is looking.
2. **Determinism** *[No intrinsic randomness]*
   We can predict the future given the present
   (modulo infinite precision and computing power).
3. **Locality** *[Local Causality]*
   No instantaneous (spooky) action at a distance.

23

23

ENTERS THE QUANTUM REALM

- *At nm length scales and mK temperatures, Nature exhibits phenomena that challenge all three pillars of the classical worldview. The Q World.*
- *Quantum mechanics describes these phenomena.*
- *At higher length or temperature scales, these phenomena get blurred, and the Q World reduces to ours.*
- *After a century of testing, quantum mechanics is our most successful theory of how the universe works.*
- *A qubit is the smallest unit of information in Q. It can be realized via electrons, photons, etc.*

24

24

The Quantum Phenomena

- **Superposition**
  A qubit can exist in 2 different states at the same time. For example, |0> + |1>
- **Collapse**
  Once measured, the qubit collapses to a bit (comes to our world) by randomly choosing 0 or 1.
- **Entanglement** *|00> + |11>*
  A two-qubit state in which collapsing one collapses the other instantly regardless of separation.
- **No Cloning**
  The state of a qubit cannot be copied.

25

25

Quantum Computing

Quantum computers are similar to classical ones in that their circuits involve wires and digital logic gates, but since they use qubits rather than bits, the values in the wires are 0 and 1, not 0 or 1. Hence, information content grows exponentially.

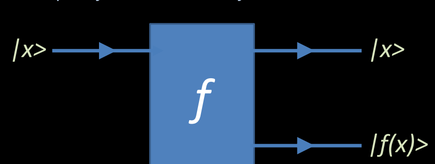
WIRES	QUANTUM STATE
1	|0> + |1>
2	(|0>+|1>)(|0>+|1>) = |00> + |01> + |10> + |11> = |0>+|1>+|2>+|3>
3	(|0>+|1>)(|0>+|1>)(|0>+|1>) = |000> + |001> + |010> + . . . + |111> = |0>+|1>+|2>+|3>+|4>+|5>+|6>+|7>
. . .	. . .
n	(|0>+|1>) (|0>+|1>) … (|0>+|1>) = |000…0> + |000…1> + . . . + |111…1> = |0> + |1> + |2> + . . . + |2^n - 1>

26

26

Quantum Computing

A logic gate takes x as input, computes a function f(x), and then outputs x and f(x). If we feed it x as n qubits in superposition, it would compute f at all 2^n values of x in one shot!



The two outputs are entangled. If you measure the upper and found it, say, x=5, then the lower would be f(5). Not useful like this because the collapse gives us only one function evaluation.

27

27

Shor's Algorithm

- Pick $f(x) = a^x \% N$
- Select a base a that is is coprime with N
- Feed m wires |x> to the function gate ($2^m > N$)
- Measure the lower output. Say you found it = F
- The upper output will collapse to a superposition of all x values whose $f(x) = F$
- The quantum circuit determines the period r of f.
- $f(r) = 1 \Rightarrow (a^{r/2} - 1)(a^{r/2} + 1) = 0$
  => *we factored N and broke RSA**!
  *May need to pick a different a if r is odd or if $a^{r/2} = -1$.

28

28

Shor's Algorithm Example

- Example: *N=21, a=2, and F = 16*
- We start with
  |0> + |1> + |2> + ...
- And end with
  |4> + |10> + |16> + |22> + ...
- From this we conclude the period r = 6
- Since 6 is even and $2^{6/2} = 8 \neq 20$, we continue
- GCD(8 −1, 21) = 7 and GCD(8+1, 21) = 3
- The factors of 21 are 3 and 7.

29

29

Other Quantum Algorithms

- Many problems can be reduced to a computation of a function f.
- The ability to compute f at *all* values of x in O(1) allows Q algorithms to extract global features and patterns in f (such as its period) quickly.
- This breaks all cryptosystems that rely on hiding these features behind long computations.
- It also speeds up the process of exhaustively trying all keys for symmetric cryptosystems.
- And fo finding pre-images of hash functions.

30

30

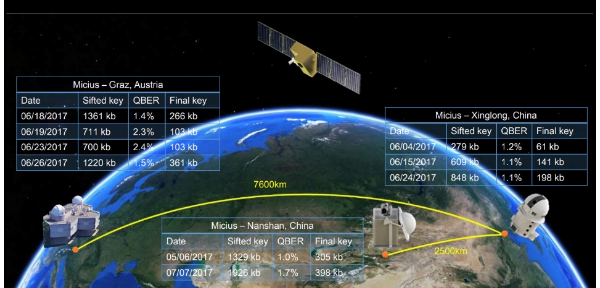
Quantum Key Distribution

- BB84 (Charles Bennett and Gilles Brassard, 1984) is a quantum protocol to establish/renew keys.
- Its strength is derived not from a computationally hard problem but from quantum properties:
- Collapse: Eve cannot sniff traffic (measure) without damaging it, thereby exposing her presence.
- No-Cloning: Eve cannot duplicate and store traffic for later processing.
- It has been implemented using photons in fiber and in space.

31

31

Qubits from China to Austria



See the q_* files in the repository.

32

32