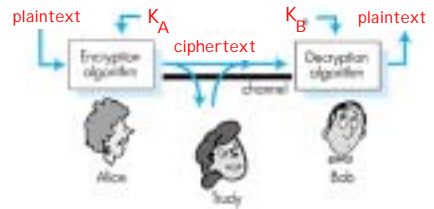


Cryptography

Advanced Topics: Public Key Cryptography,
Quantum Cryptography

The language of cryptography



symmetric key crypto: sender, receiver keys identical

public-key crypto: encrypt key *public*, decrypt key *secret*

Symmetric key cryptography

substitution cipher: substituting one thing for another

– monoalphabetic cipher: substitute one letter for another

plaintext: abcdefghijklmnopqrstuvwxyz

ciphertext: mnbvcxzasdfghjklpoiuytrewq

E.g.: Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc

Q: [How hard to break this simple cipher?:](#)

- brute force (how hard?)
- other?

Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64 bit plaintext input
- How secure is DES?
 - DES Challenge: 56-bit-key-encrypted phrase (“Strong cryptography makes the world a safer place”) decrypted (brute force) in 4 months
 - no known “backdoor” decryption approach
- making DES more secure
 - use three keys sequentially (3-DES) on each datum
 - use cipher-block chaining

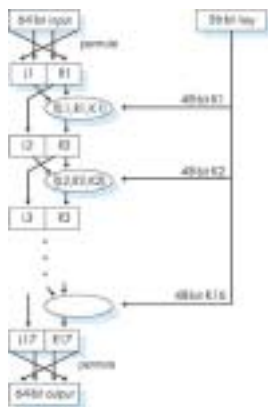
Symmetric key crypto: DES

DES operation

initial permutation

16 identical “rounds” of function application, each using different 48 bits of key

final permutation



Public Key Cryptography

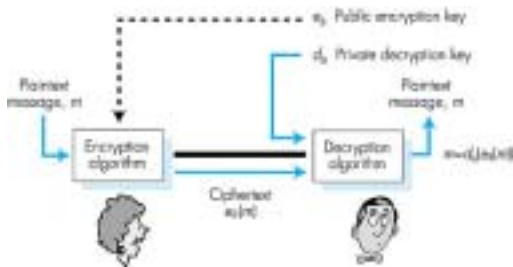
symmetric key crypto

- requires sender, receiver know shared secret key
- Q: how to agree on key in first place (particularly if never “met”)?

public key cryptography

- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- encryption key *public* (known to *all*)
- decryption key *private* (known only to receiver)

Public key cryptography



Digital Signatures

Cryptographic technique analogous to hand-written signatures.

- Sender (Bob) digitally signs document, establishing he is document owner/creator.
- **Verifiable, nonforgeable:** recipient (Alice) can verify that Bob, and no one else, signed document.

Simple digital signature for message m :

- Bob encrypts m with his private key d_B , creating signed message, $d_B(m)$.
- Bob sends m and $d_B(m)$ to Alice.



Digital Signatures (more)

- Suppose Alice receives msg m , and digital signature $d_B(m)$
 - Alice verifies m signed by Bob by applying Bob's public key e_B to $d_B(m)$ then checks $e_B(d_B(m)) = m$.
 - If $e_B(d_B(m)) = m$, whoever signed m must have used Bob's private key.
- Alice thus verifies that:**
- Bob signed m .
 - No one else signed m .
 - Bob signed m and not m' .
- Non-repudiation:**
- Alice can take m , and signature $d_B(m)$ to court and prove that Bob signed m .

Message



Computationally expensive to public-key-encrypt long messages

- Goal:** fixed-length, easy to compute digital signature, "fingerprint"
- apply hash function H to m , get fixed size message digest, $H(m)$.

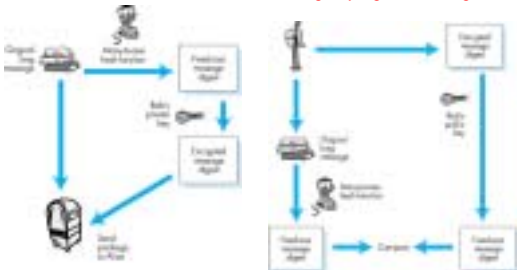
Hash function properties:

- Many-to-1
- Produces fixed-size msg digest (fingerprint)
- Given message digest x , computationally infeasible to find m such that $x = H(m)$
- computationally infeasible to find any two messages m and m' such that $H(m) = H(m')$.

Digital signature = Signed message digest

Bob sends digitally signed message:

Alice verifies signature and integrity of digitally signed message:



Hash Function Algorithms

- **Internet checksum would make a poor message digest.**
 - Too easy to find two messages with same checksum.
- **MD5 hash function widely used.**
 - Computes 128-bit message digest in 4-step process.
 - arbitrary 128-bit string x , appears difficult to construct msg m whose MD5 hash is equal to x .
- **SHA-1 is also used.**
 - US standard
 - 160-bit message digest

Quantum Computing

- **Basic Premise: Superposition of state.**
 - A particle may exist in multiple distinct states at the same time.
 - Young's double slit diffraction experiment yields a fringe pattern, which shows the wave nature of light.
 - The same fringe pattern is observed in a double slit experiment even when a single photon is emitted.
- **Quantum Computing**
 - The basic unit of state is a qubit.
 - Exists as a superposition of state.
 - Spin is a common state variable used to represent a qubit
 - Observation: A 4 bit number has one of 16 possible values. A 4 qubit number has *all* 16 values simultaneously.

Quantum Computing

- A quantum computer can represent all values of state variables simultaneously.
 - This is exploited by quantum algorithms, which execute simultaneously on all possible inputs.
- A quantum computer is exponentially faster than current day computers.
- NP hard problems can be solved in linear time in a quantum computer.
- **Effect: Prime factorization is not a hard problem any more.**
 - Shor's algorithm computes prime numbers in linear time (Peter Shor, 1994 AT&T Bell Labs). Breaks RSA.
 - Grover's algorithm generates permutations in linear time. (Lov Grover, 1996 AT&T Bell Labs). Breaks DES

Quantum Money

- **Idea: Measuring polarization of a single photon is inherently unreliable. The operation is also destructive. (Wiesner)**
- Uses 4 possible polarizations.
- Currency has a serial number and a set of 20 light traps, each containing a single photon.
- Bank knows the correspondence between the serial number and the sequence of polarized photons.
 - Counterfeiter can't determine the polarization. Hence it is impossible to produce counterfeit currency with the correct match between polarization and serial number.
- This idea is the basis for quantum cryptography.
 - Bennet and Brassard (IBM TJ Watson, Univ. of Montreal)

Quantum Cryptography

- Alice has 2 possible polarization formats + (rectilinear) or x (diagonal)
- Randomly chooses the polarization format
- Each bit of the original message is encoded in the chosen polarization format.
- Eve (the intruder) cannot decode the message, since she doesn't know the polarization format.
 - For instance if the original bit – say 1 – was encoded in the + format and Eve uses the x format, she cannot tell if the bit is a 1 or a 0, since 1 in the + format may or may not pass through a x polaroid.
 - If Eve can't even read the message, there is no point in trying to decrypt.

Quantum Cryptography

- **Problem: Bob (the intended recipient) can't read the message either.**
- **Solution:**
 - Alice can share the sequence of polarizations she uses with Bob (shared symmetric key)
 - Issue: We are back to the key distribution problem.
 - Can't rely on public key cryptography for key dissemination. Remember quantum computers.

Quantum Cryptography

- Three phase algorithm
- Alice transmits a random sequence of bits using a random choice of + or x formats
- Bob measures the polarization and hence the value of the bits using essentially a random choice of polarization formats
- Alice calls Bob and tells him her choice of polarization formats. Bobs tells her which choices he got right. Alice and Bob use the bit string of right choices as a one time cipher.
- Note: One time ciphers are absolutely unbreakable.

Why does it work?

- Intuition: Eve knows the polarization formats after the fact. She still doesn't know the data values, which were never discussed.
 - For instance, Alice sends a 1 using the + format.
 - Eve uses a x polaroid, so she ends up with a 1 or a 0 corresponding to the original 1.
 - Later Alice indicates that she used the + format.
 - Eve still can't tell if the data bit was a 1 or a 0. Basically the knowledge of the polarization format arrived too late to be of use to Eve.
- How about data corruption?
 - Eve's use of a polaroid modifies the polarization of the transmitted photon stream. This will affect Bob's readings

Detecting the (Eve)sdropper

- The problem with data corruption is the Alice cannot be sure that Bob has the right data bits, even though Bob got the polarization right.
 - For instance Alice uses the x format to send a 1. Eve uses the + format. If the 1 gets through and Bob uses the right x detector, he will still end up with a 0 or a 1.
- Solution:
 - Bob maintains the list of correct polarization choices he made. So theoretically, he should have the correct bit pattern for the correct polarization choices.
 - Alice reads out a smaller random subset of the correct bit pattern. If any of the bits in the subset are wrong in Bob's list, they detect the intruder.
 - Alice and Bob discard the bits they just discussed.

Current State of the Art

- First implementation: Communication over 30 cm. (Bennet 1988)
- Univ of Geneva: Photons over fibre.
 - QC over a distance of 23 km
- Los Alamos is working on satellite communication over quantum cryptography.
- Quantum cryptography is considered to be theoretically unbreakable, since it would defy quantum mechanics as we know it.