Fundamentals of Cryptography

David Jao

Topics in Quantum-Safe Cryptography

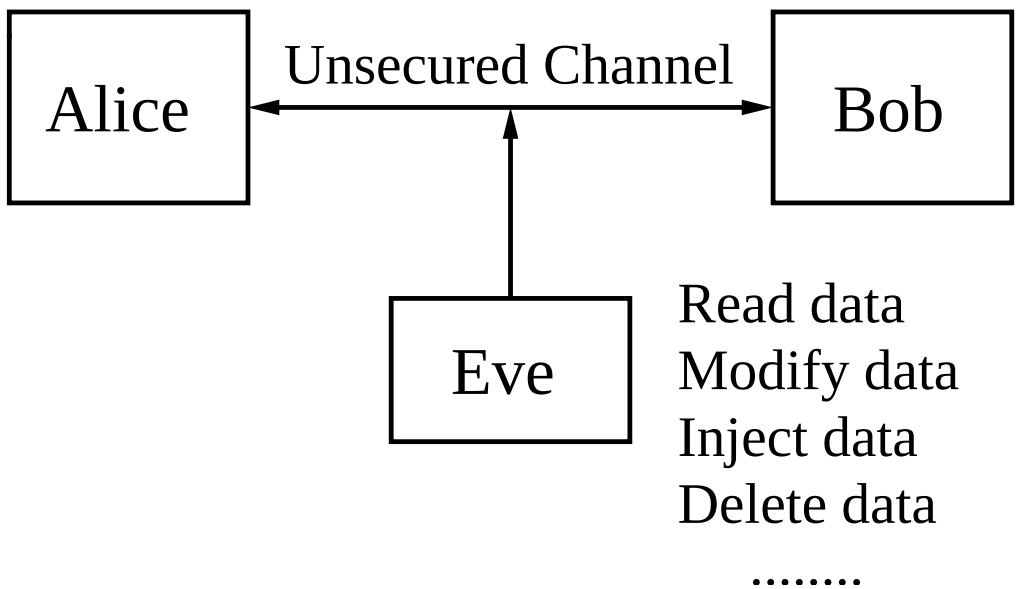
CryptoWorks21

UNIVERSITY OF
WATERLOO

June 21, 2016

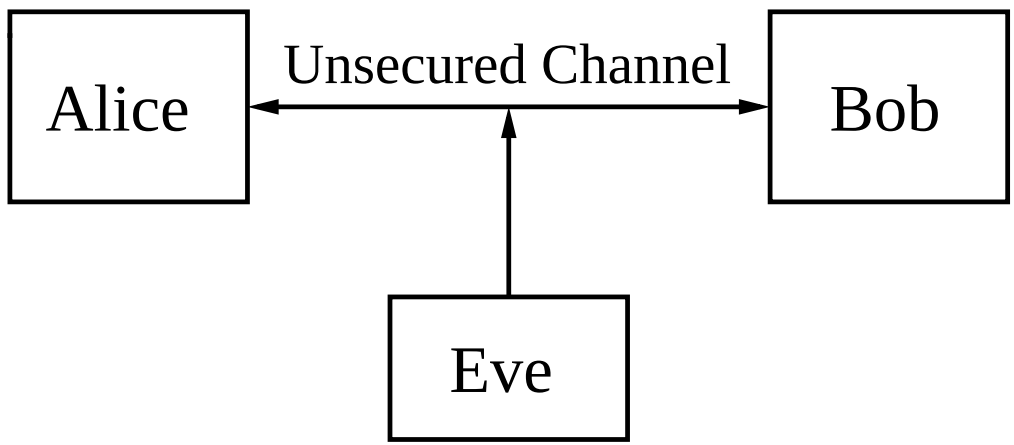
What is cryptography?

Cryptography is about securing communication in the presence of malicious adversaries.



Fundamental goals of cryptography

- Confidentiality: Keep data secret from all but those authorized to see it
- Data integrity: Ensure data has not been altered by unauthorized means
- Data origin authentication: Corroborate the source of data
- Non-repudiation: Prevent an entity from denying previous commitments or actions



Cryptography vs. security

Information security encompasses the concepts, techniques, technical measures, and administrative measures used to protect information assests from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

The real challenge is an engineering one: building high confidence systems which

- Behave in a well-understood and predictable fashion
- Withstand malicious attacks as well as naturally occurring hazards
- Must not cause or contribute to accidents or unacceptable losses

Cryptography vs. security

Information security includes the study of subjects like:

- Computer security
- Network security
- Software security

Cryptography $\neq$ Security

- Cryptography provides some mathematical tools that can assist with the provision of information security services. It is a small but essential part of a complete solution.
- Security is a chain
  - Weak links become targets
  - One flaw is all it takes (Door locks $\neq$ Home security)
  - Cryptography is usually not the weakest link (however, when the crypto fails the damage can be catastrophic)

Part I

Symmetric key cryptosystems

Basic concepts

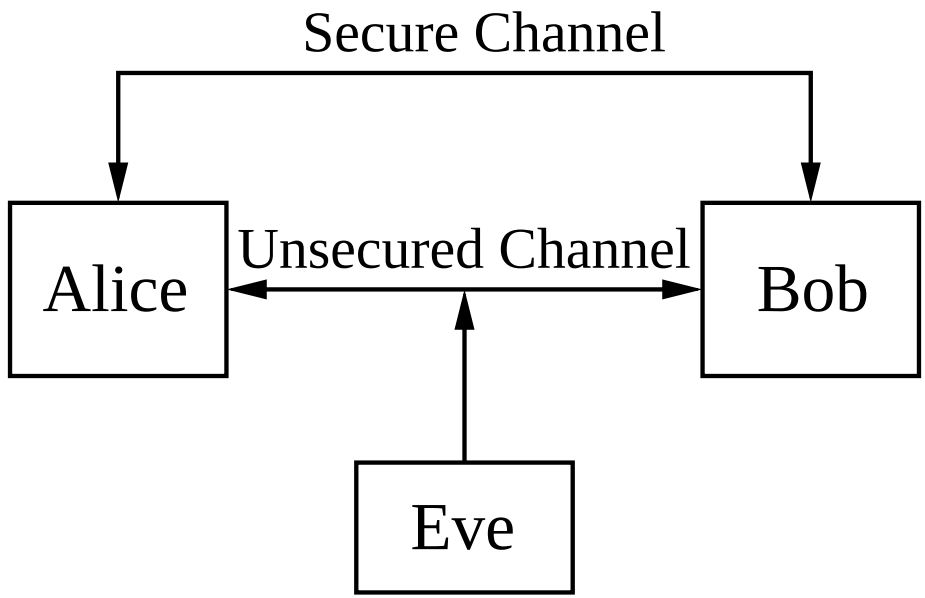
Definition: A symmetric-key encryption scheme (SKES) consists of:

- M – the plaintext space,
- C – the ciphertext space,
- K – the key space,
- a family of encryption functions, $E_k \colon M \to C$, $\forall k \in K$,
- a family of decryption functions, $D_k \colon C \to M$, $\forall k \in K$,

such that $D_k(E_k(m)) = m$ for all $m \in M$, $k \in K$.

Equivalently: $E \colon K \times M \to C$ and $D \colon K \times C \to M$.

Using a SKES to achieve confidentiality



1. Alice and Bob agree on a secret key $k \in K$ by communicating over the secure channel.
2. Alice computes $c = E_k(m)$ and sends the ciphertext c to Bob over the unsecured channel.
3. Bob retrieves the plaintext by computing $m = D_k(c)$.

Substitution cipher

The substitution cipher is defined to be the following SKES.

- M = all English messages.
- C = all encrypted messages.
- K = all permutations of the English alphabet.
- $E_k(m)$: Apply permutation k to m, one letter at a time.
- $D_k(c)$: Apply inverse permutation k^{-1} to c, one letter at a time.

Example:

$k =$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	N	X	E	S	K	O	J	T	A	F	P	Y	I	Q	U	B	R	Z	G	V	C	H	M	W	L

$m =$ the big dog, $\quad c = E_k(\text{the big dog}) =$ GJS NTO EQO.

Question: Is the simple substitution cipher a secure SKES?

Polyalphabetic Ciphers

Basic idea: Use several permutations, so a plaintext letter is encrypted to one of several possible ciphertext letters.

Example: Vigenère cipher:

- Key is an English word having no repeated letters
  e.g. $k = \text{CRYPTO}$.
- Example of encryption:

$m =$	t	h	i	s		i	s		a	m	e	s	s	a	g	e
$+\ k =$	C	R	Y	P		T	O		C	R	Y	P	T	O	C	R
$c =$	V	Y	G	H		B	G		C	D	C	H	L	O	I	V

- Here, A=0, . . ., Z=25; addition of letters is mod 26.
- Decryption is subtraction modulo 26.
- Frequency distribution of ciphertext letters is flatter (than for a simple substitution cipher).

The One-Time Pad

The One-Time Pad is a modified version of the Vigenère cipher.

- Invented by Vernam in 1917 for the telegraph system
- Key is a random string of letters
- Example of encryption:

$m =$	t	h	i	s	i	s	a	m	e	s	s	a	g	e
$+ k =$	Z	F	K	W	O	G	P	S	M	F	J	D	L	G
$c =$	S	M	S	P	W	Y	P	F	Q	X	C	D	R	K

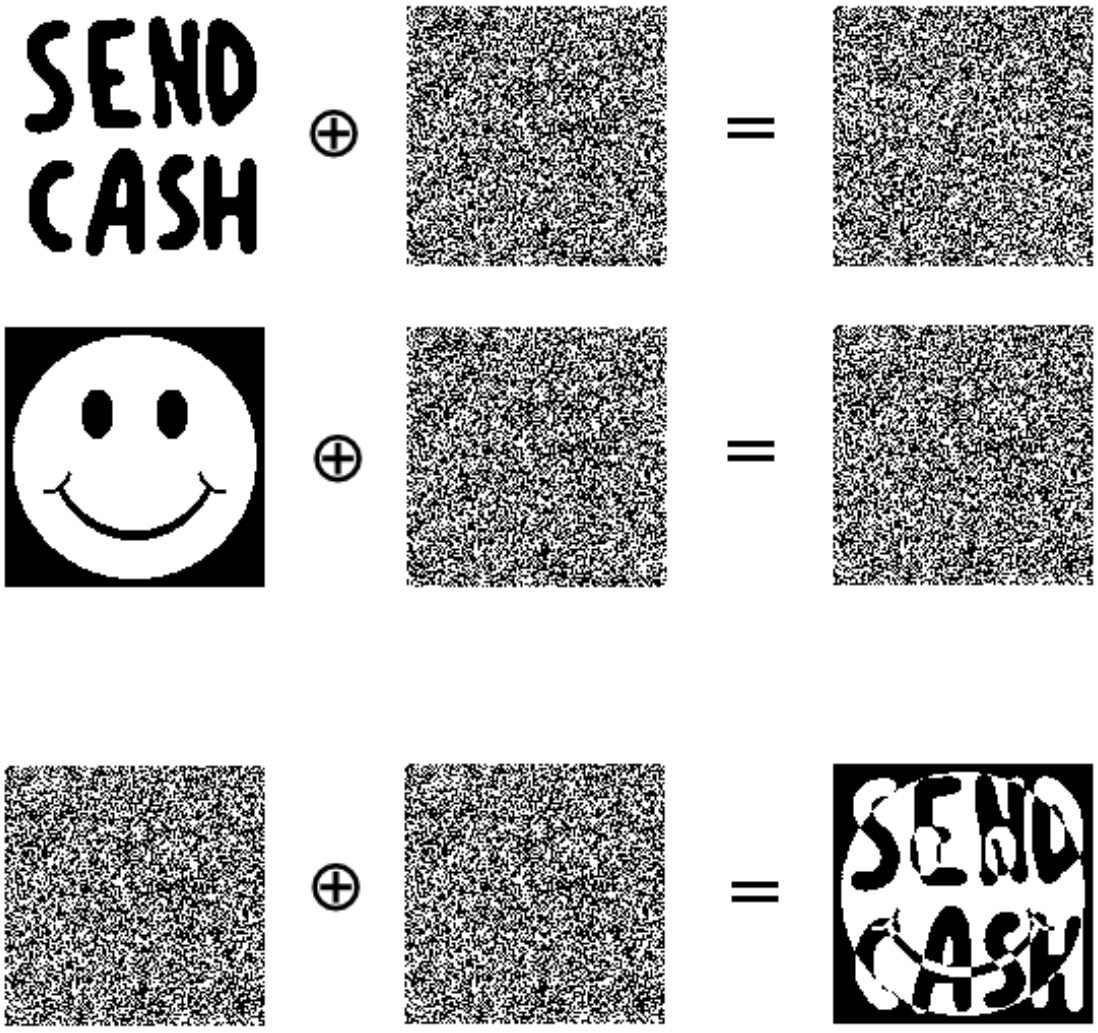
- Note: The key is as long as the plaintext.

Re-use of One-Time Pads

The key should not be re-used:

- If $c_1 = m_1 + k$ and $c_2 = m_2 + k$, then $c_1 - c_2 = m_1 - m_2$.
- $c_1 - c_2$ depends only on the plaintext (and not on the key) and hence can leak information about the plaintext.
- If m_1 is known, then m_2 can be easily computed.

Re-use of One-Time Pads



(Source: `http://www.cryptosmith.com/archives/70`)

What Does it Mean for a SKES to be Secure?

Three key questions:

1. How does the adversary interact with the communicating parties?
2. What are the computational powers of the adversary?
3. What is the adversary's goal?

- Basic assumption: The adversary knows everything about the SKES, except the particular key k chosen by Alice and Bob. (Avoid security by obscurity!!)

- Security model: Defines the computational abilities of the adversary, and how she interacts with the communicating parties.

1. Adversary's Interaction

- Passive attacks:
  - Ciphertext-only attack.
  - Known-plaintext attack: The adversary also knows some plaintext and the corresponding ciphertext.
- Active attacks:
  - Chosen-plaintext attack: The adversary can also choose some plaintext(s) and obtain the corresponding ciphertext(s).
  - Chosen-ciphertext attack: The adversary can also choose some ciphretext(s) and obtain the corresponding plaintext(s).
- Other attacks:
  - Side-channel attacks: monitor the encryption and decryption equipment (timing attacks, power analysis attacks, electromagnetic-radiation analysis, etc.)
  - Physical attacks: bribery, blackmail, rubber hose, etc.

2. Computational Power of the Adversary

- Information-theoretic security: Eve has infinite computational resources.
- Complexity-theoretic security: Eve is a "polynomial-time Turing machine".
- Computational security: Eve has X number of real computers/workstations/supercomputers. (Eve is "computationally bounded")

Adversary's Goal

1. Recover the secret key.
2. Systematically recover plaintext from ciphertext (without necessarily learning the secret key).
3. Learn some partial information about the plaintext from the ciphertext (other than its length).

- If the adversary can achieve 1 or 2, the SKES is said to be totally insecure (or totally broken).
- If the adversary cannot learn any partial information about the plaintext from the ciphertext (except possibly its length), the SKES is said to be semantically secure.

Hiding length information is very hard. This topic falls under the heading of *traffic analysis*.

Definition of a Secure SKES

Definition

A symmetric-key encryption scheme is said to be secure if it is semantically secure against a chosen-plaintext attack by a computationally bounded adversary.

To break a symmetric-key encryption scheme, the adversary has to accomplish the following:

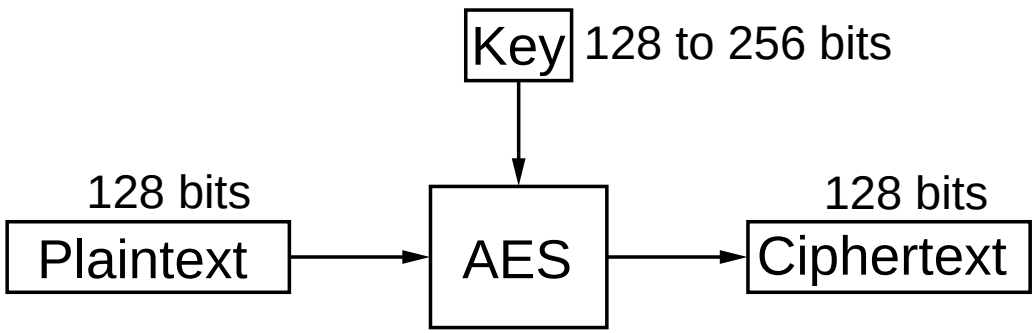
1. The adversary is given a challenge ciphertext c (generated by Alice or Bob using their secret key k).
2. During its computation, the adversary can select plaintext and obtains (from Alice or Bob) the corresponding ciphertext.
3. After a feasible amount of computation, the adversary obtains some information about the plaintext corresponding to c (other than the length of m).

Part II

Block ciphers

Block ciphers and stream ciphers

- A block cipher is a SKES which breaks up the plaintext into blocks of a fixed length (e.g. 128 bits), and encrypts the blocks one at a time.
- In contrast, a stream cipher encrypts the plaintext one character (usually a bit) at a time.
- Example of a block cipher:
  The Advanced Encryption Standard (AES)



Key size: 128 to 256 bits; Size of key space: 2^{128} to 2^{256};
Block size: 128 bits.

20th-century history of symmetric-key encryption schemes

- One-time pad (Vernam, 1917)
- Electro-mechanical (stream) ciphers of World War II:
  - Enigma (Germany)
  - Lorenz (Germany)
  - PURPLE (Japan)
  - Navajo code (USA)
- Late 1960's: Feistel network, substitution-permutation network, and LUCIFER designed at IBM.

20th-century history of symmetric-key encryption schemes

- 1972: NBS (now NIST: National Institute of Standards and Technology) solicits proposals for encryption algorithms for the protection of computer data.
- 1974: IBM submits a variant of Lucifer (based on a Feistel network) as a DES candidate.
- 1975: NSA (National Security Agency) (allegedly) "fixes" DES
  - Reduces the key size from 64 bits to 56 bits.

    "We sent the S-boxes off to Washington. They came back and were all different."
- 1977: DES adopted as US Federal Information Processing Standard (FIPS 46).
- 1981: DES adopted as a US banking standard (ANSI X3.92).

21st-century history of symmetric-key encryption schemes

- 1997: NIST begins the AES (Advanced Encryption Standard) competition.
- 1999: 5 finalists for AES announced.
- 2001: Rijndael adopted for AES (FIPS 197).
  - AES has three key sizes: 128, 192 and 256 bits.
  - Based on a substitution-permutation network design
- 2012:
  - No significant weaknesses found with AES (as yet).
  - AES is in widespread use.
  - DES (and Triple-DES) is declining in usage but still widely deployed.

The Advanced Encryption Standard (AES)

- `www.nist.gov/aes`
- Sept. 1997: Call issued for AES candidate algorithms.
- Requirements:
  - Key sizes: 128, 192 and 256 bits.
  - Block size: 128 bits.
  - Efficient on both hardware and software platforms.
  - Availability on a worldwide, non-exclusive, royalty-free basis.

The AES process

- Aug. 1998: 15 submissions in Round 1.
- Aug. 1999: NIST selects five finalists:
  - MARS, RC6, Rijndael, Serpent, Twofish.
- 1999: NSA performs a hardware efficiency comparison.
- Oct. 2, 2000: Rijndael is selected.
- Dec. 2001: The AES standard is officially adopted (FIPS 197).
- Rijndael is an iterated block cipher. It is a substitution-permutation network, not a Feistel cipher.

Advanced Encryption Standard

- AES is a substitution-permutation network where the "permutation" operation consists of two linear transformations (one of which is a permutation).
- All operations are byte oriented (e.g., S-box maps 8-bits to 8-bits). This allows AES to be efficiently implemented on various platforms.
- The block size of AES is 128 bits.
- Each round key is 128 bits.
- AES accepts three different key lengths. The number of rounds depends on the key length:

key length	h
128	10
192	12
256	14