Cryptography (and Information Security)
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 2.1: General cryptographic schema

Motivation then and now

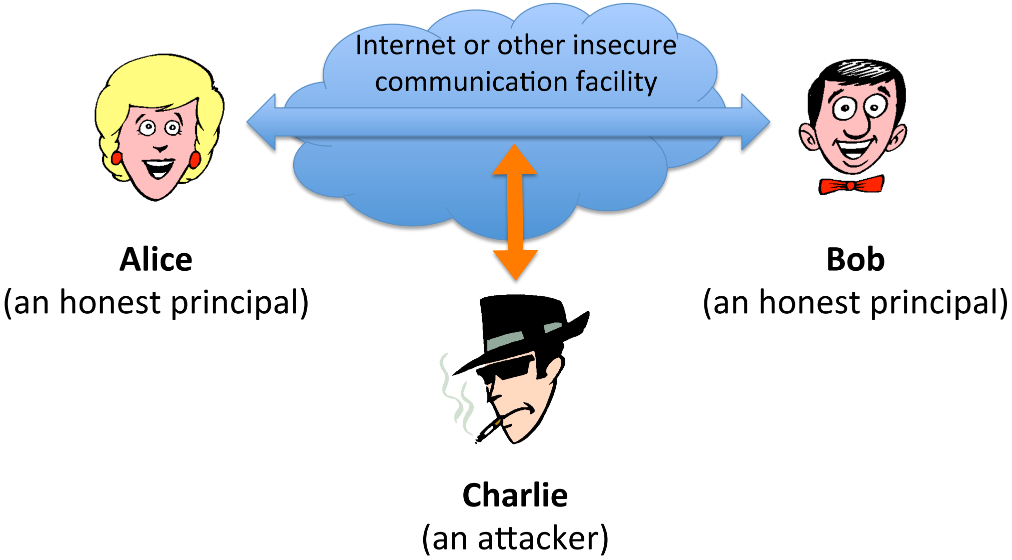
Three can keep a secret, if two of them are dead.

— Benjamin Franklin

We interact and transact by directing flocks of digital packets towards each other through cyberspace, carrying love notes, digital cash, and secret corporate documents. Our personal and economic lives rely on our ability to let such ethereal carrier pigeons mediate at a distance what we used to do with face-to-face meetings, paper documents, and a firm handshake. How do we converse privately when every syllable is bounced off a satellite and smeared over an entire continent? How should a bank know that it really is Bill Gates requesting from his laptop in Fiji a transfer of $10,000,000,000 to another bank? Fortunately, the mathematics of cryptography can help.

— Ron Rivest

What’s it all about?

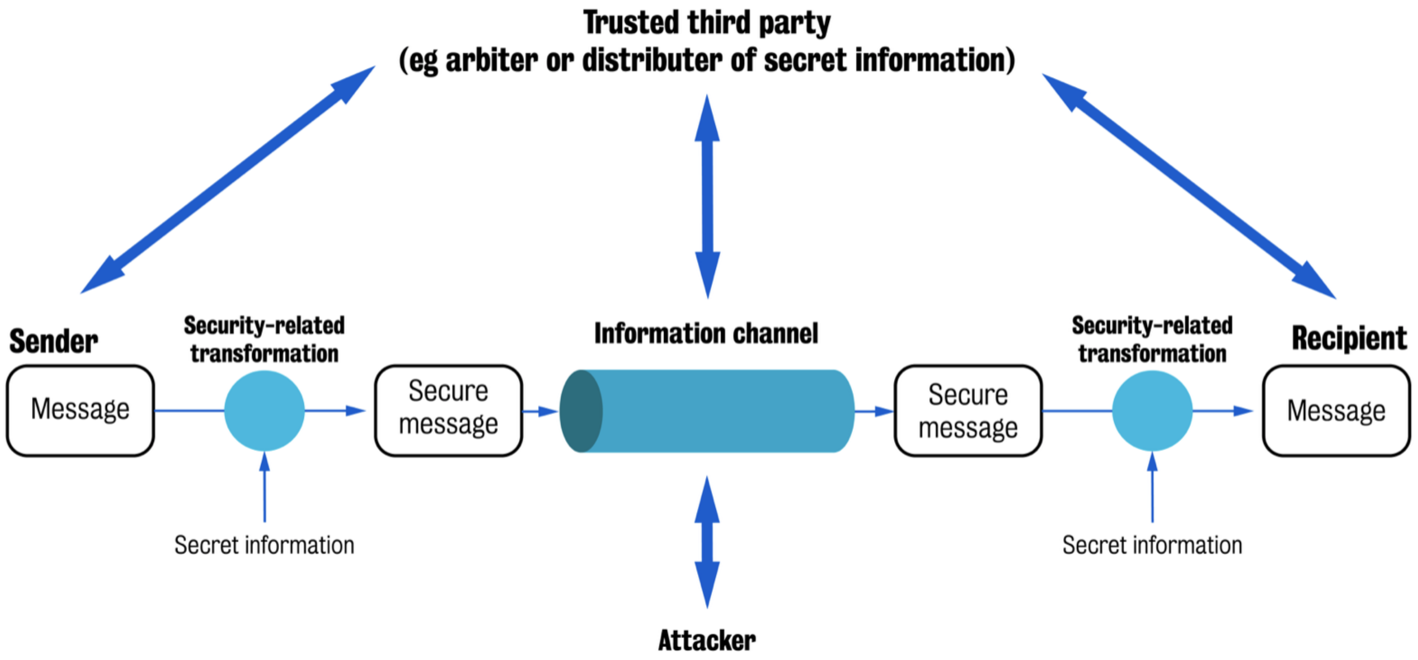


How do we turn an insecure communication facility (like the Internet) into a secure one?

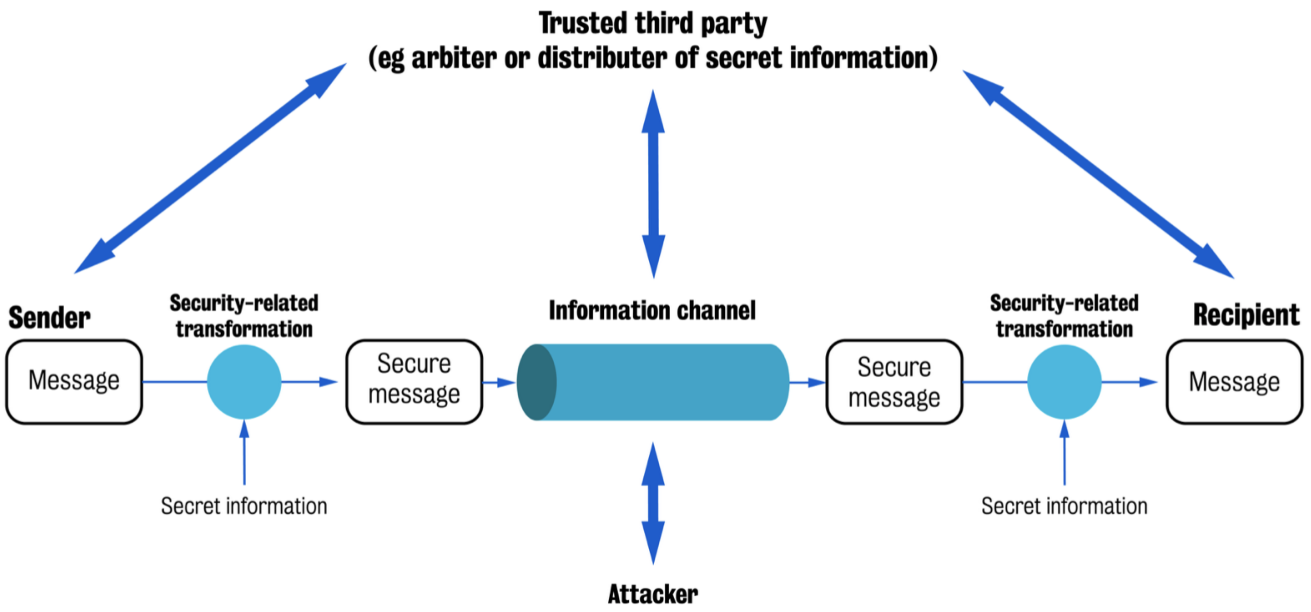
Where security means that one or more security properties (e.g., confidentiality, integrity, authentication, non-repudiation, anonymity, unobservability, timeliness, availability, etc.) are guaranteed.

Cryptography is the enabling technology.

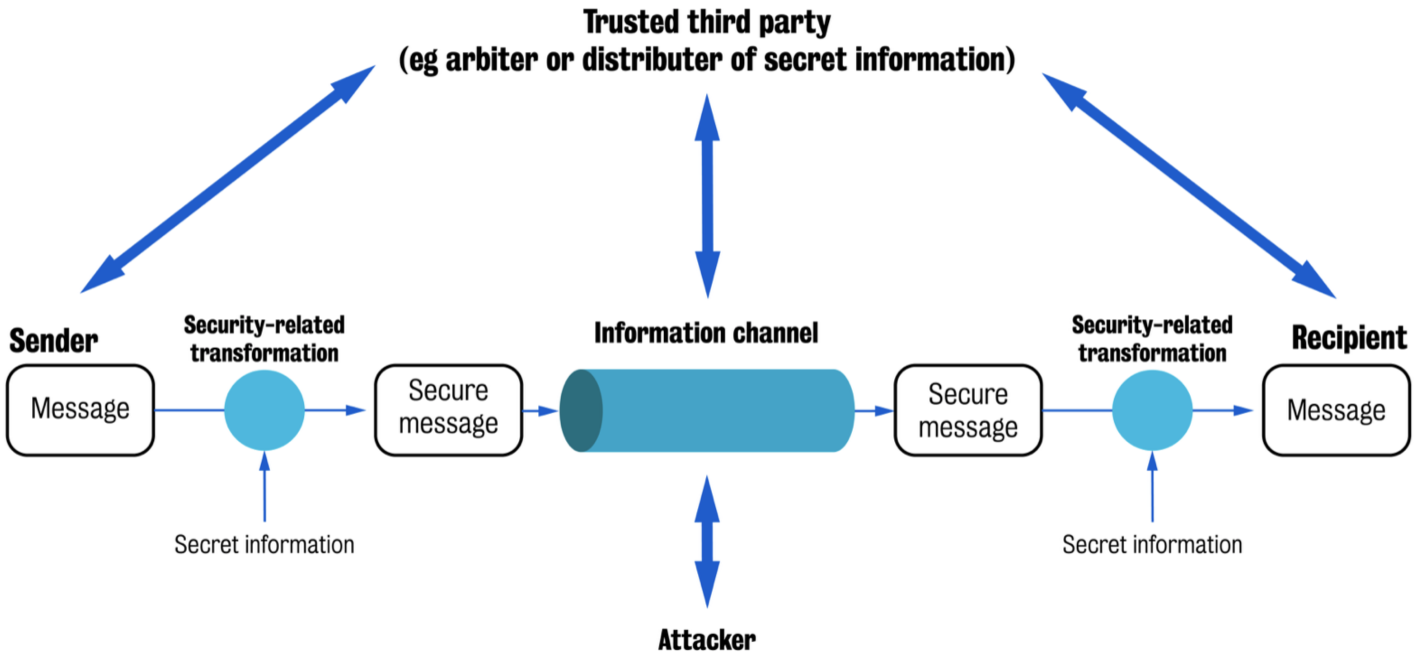
A general model for (network) security



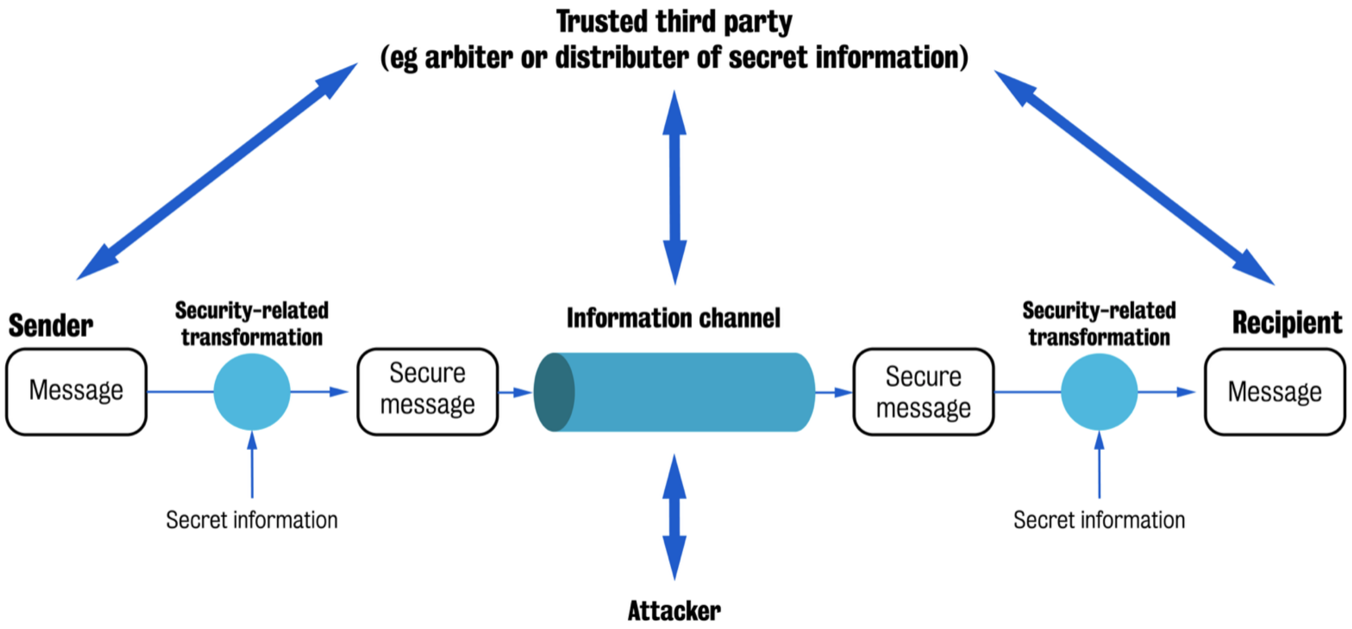
- A **message** is to be transferred **from one principal (Sender) to another (Recipient)** across some sort of Internet service.
- The two principals must cooperate for the exchange to take place.
- A logical **information channel** is established by defining a route through Internet from source to destination and by principals' cooperative use of communication protocols (e.g., TCP/IP).



- All the techniques for providing security have two components:
  1. A **security-related transformation** on information to be sent, e.g.
     - **encryption** of the message, which “scrambles” the message so that it is unreadable by the opponent, and/or
     - addition of a **code** based on the contents of the message, which can be used to verify the identity of the sender (e.g., MAC or MDC).
  2. Some **secret information** shared by the two principals and, it is hoped, unknown to the opponent, e.g.
     - **encryption key** used in conjunction with transformation to “scramble” message before transmission and unscramble it on reception.

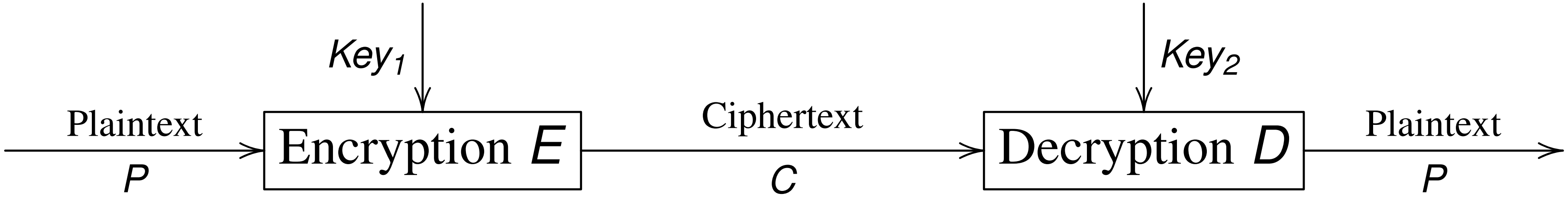


- A **trusted third party** may be needed to achieve secure transmission, e.g.
  - responsible for distributing the secret information to the two principals while keeping it from any opponent, or
  - needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.



- This general model shows that there are **4 basic tasks**:
  1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.
  4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

General cryptographic schema



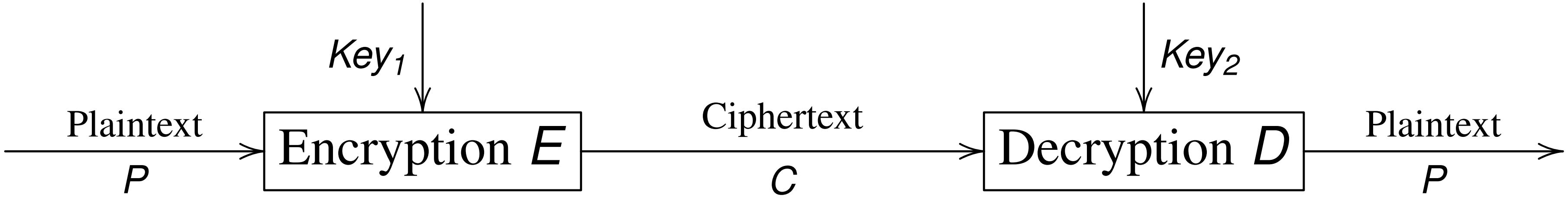
where $E(Key_1, P) = C$ and $D(Key_2, C) = P$.

Terminology

- **Plaintext** (or **plain text**, **clear text**, ...): text that can be read and “understood” (e.g., by a human being).
- **Encryption**: transformation (or function, process, procedure, ...) E that takes in input a plaintext and a key and generates a ciphertext.
- **Ciphertext** (or **cipher text**, **encrypted text**, ...): transformed (or “scrambled”, ...) text that needs to be “processed” to be “understood” (e.g., by a human being).
- **Decryption**: transformation (or function, process, procedure, ...) D that takes in input a ciphertext and a key and generates a plaintext.

Cipher: a function (or algorithm, ...) for performing encryption/decryption.

General cryptographic schema



where $E(Key_1, P) = C$ and $D(Key_2, C) = P$.

- **Symmetric algorithms**:
  - $Key_1 = Key_2$, or are easily derived from each other.
- **Asymmetric (or public key) algorithms**:
  - Different keys, which cannot be derived from each other.
  - Public key can be published without compromising private key.
- Encryption and decryption should be easy, if keys are known.
- **Security depends only on secrecy of the key, not on the algorithm.**

Kerckhoffs' "La Cryptographie Militaire"

Security depends only on secrecy of the key, not on the algorithm.

J.-G.-H.-V.-F.-A.-A. Kerckhoffs von Nieuwenhof, "La Cryptographie Militaire" in Journal des sciences militaires, vol. IX, 1883 (!)

Six fundamental principles for military ciphers:

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable.
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
4. Il faut qu'il soit applicable à la correspondance télégraphique.
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Kerckhoffs' "La Cryptographie Militaire"

Security depends only on secrecy of the key, not on the algorithm.

J.-G.-H.-V.-F.-A.-A. Kerckhoffs von Nieuwenhof, "La Cryptographie Militaire" in Journal des sciences militaires, vol. IX, 1883 (!)

Six fundamental principles for military ciphers:

1. The system must be substantially, if not mathematically, undecipherable.
2. **The system must not be required to be secret and can be stolen by the enemy without causing trouble.**
3. It must be easy to communicate and retain the key without the aid of written notes, it must also be easy to change or modify the key at the discretion of the correspondents.
4. The system ought to be compatible with telegraph communication.
5. It must be portable, and its use must not require more than one person.
6. Finally, given the circumstances in which such system is applied, it must be easy to use and must neither stress the mind or require the knowledge of a long series of rules.

A simple example

- Map each letter to a number:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Define:

$$C = E(K,P) = (P+K) \bmod 26$$
$$P = D(K,C) = (C-K) \bmod 26$$

- Pick, say, $K = 3$ so that $C = E(3,P) = (P+3) \bmod 26$
- If $P =$ “H”
  then $C = E(3,7) = (7+3) \bmod 26 = 10 \bmod 26 = 10 =$ “K”
- If $P =$ “Y” then $C = (24+3) \bmod 26 = 27 \bmod 26 = 1 =$ “B”
- Hence, if full plaintext is “HEYYOU”, then ciphertext is “KHBBRX”
- How difficult is to encrypt?
- And to decrypt? What if ciphertext is “KHOOR ZRUOG”? (space is extra information)
- And what if ciphertext is “L WRSL QRQ DYHYDQR QLSRWL”?

A simple example... but still in use

- Might look very simple, but still used in some form today.
- For instance, Bernardo Provenzano (1933–2016), accused of being the “capo di tutti capi” of the Sicilian mafia, was captured after eluding the police for over forty years.
- Provenzano was caught after police intercepted messages between Provenzano and other members of his organization written in a cipher that they were able to break:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24