2550 Intro to cybersecurity

L3

abhi shelat

Security failures

Operation

Implementation

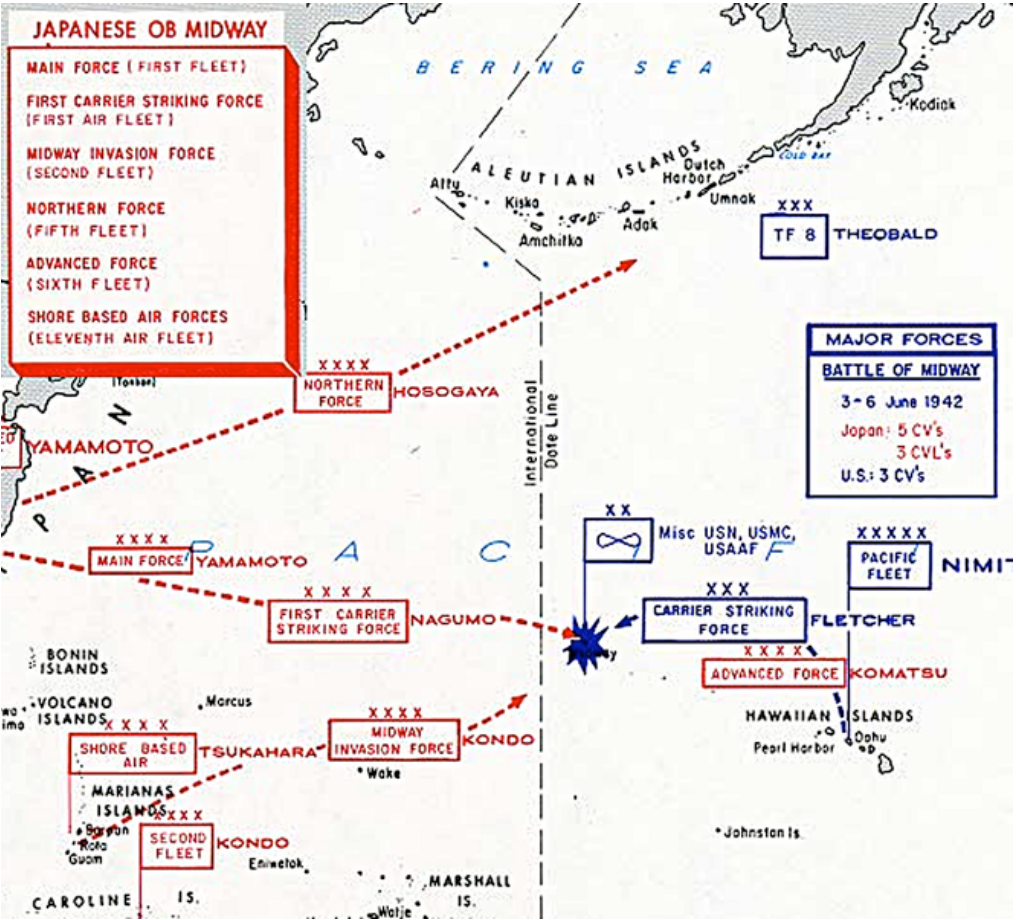
Design

Abstraction

A Network is a public resource.

Confidentiality

Goal: add privacy to a public resource.


JAPANESE OB MIDWAY
MAIN FORCE (FIRST FLEET)
FIRST CARRIER STRIKING FORCE (FIRST AIR FLEET)
MIDWAY INVASION FORCE (SECOND FLEET)
NORTHERN FORCE (FIFTH FLEET)
ADVANCED FORCE (SIXTH FLEET)
SHORE BASED AIR FORCES (ELEVENTH AIR FLEET)
BERING SEA
Kodiak
ALEUTIAN ISLANDS
Dutch Harbor
Umnak
Attu
Kiska
Amchitka
Adak
XXX
TF 8
THEOBALD
MAJOR FORCES
BATTLE OF MIDWAY
3-6 June 1942
Japan: 5 CV's
3 CVL's
U.S.: 3 CV's
XXXX
NORTHERN FORCE
HOSOGAYA
YAMAMOTO
International Date Line
XX
Misc USN, USMC, USAAF
XXXXX
PACIFIC FLEET
NIMI
XXXX
MAIN FORCE
YAMAMOTO
XXXX
FIRST CARRIER STRIKING FORCE
NAGUMO
XXX
CARRIER STRIKING FORCE
FLETCHER
XXXX
ADVANCED FORCE
KOMATSU
BONIN ISLANDS
VOLCANO ISLANDS
Marcus
XXXX
SHORE BASED AIR
TSUKAHARA
XXXX
MIDWAY INVASION FORCE
KONDO
Wake
HAWAIIAN ISLANDS
Pearl Harbor
Oahu
MARIANAS ISLANDS
XXX
SECOND FLEET
KONDO
Saipan
Rota
Guam
Eniwetok
Johnston Is
MARSHALL IS.
CAROLINE IS.
Wotje

Midway

KERCKHOFF

JOURNAL
DES
SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

KERCKHOFF

II.

DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

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.

Tout le monde est d'accord pour admettre la raison d'être des

KERCKHOFF

II.

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 ;

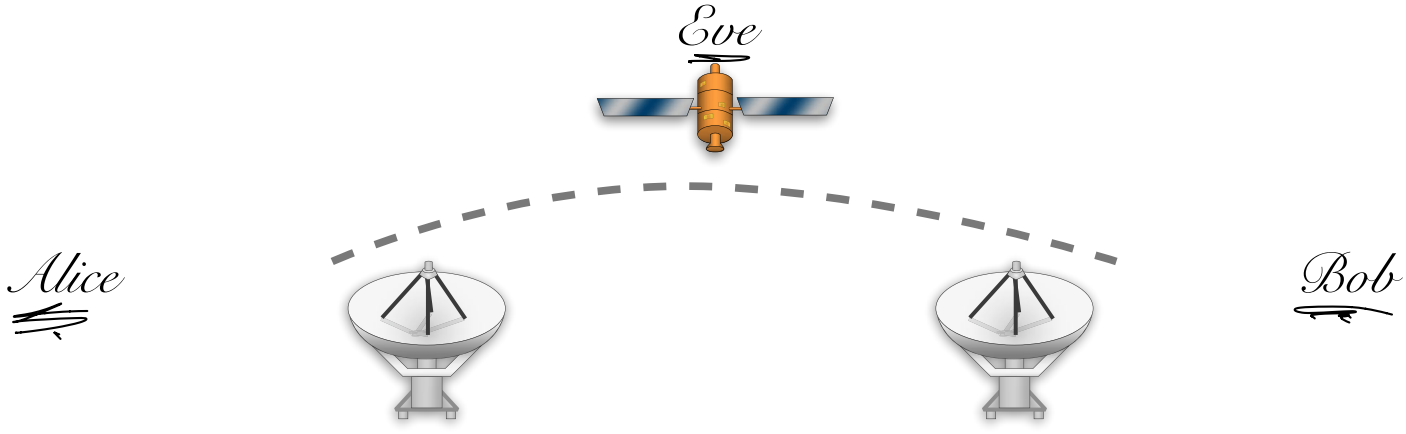
5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

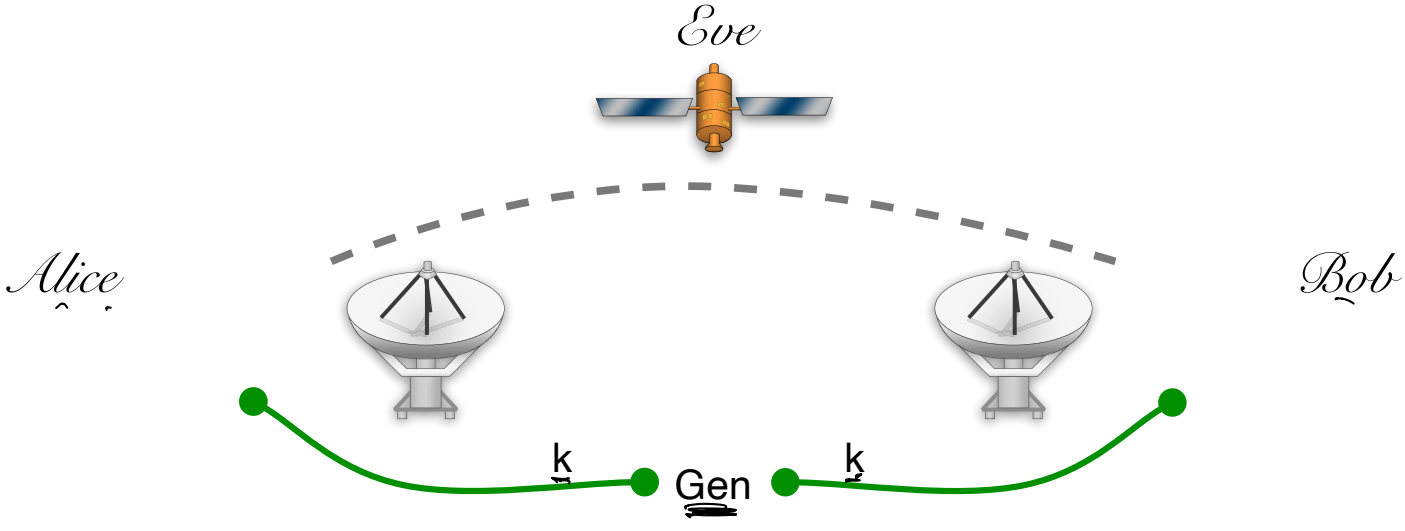
6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

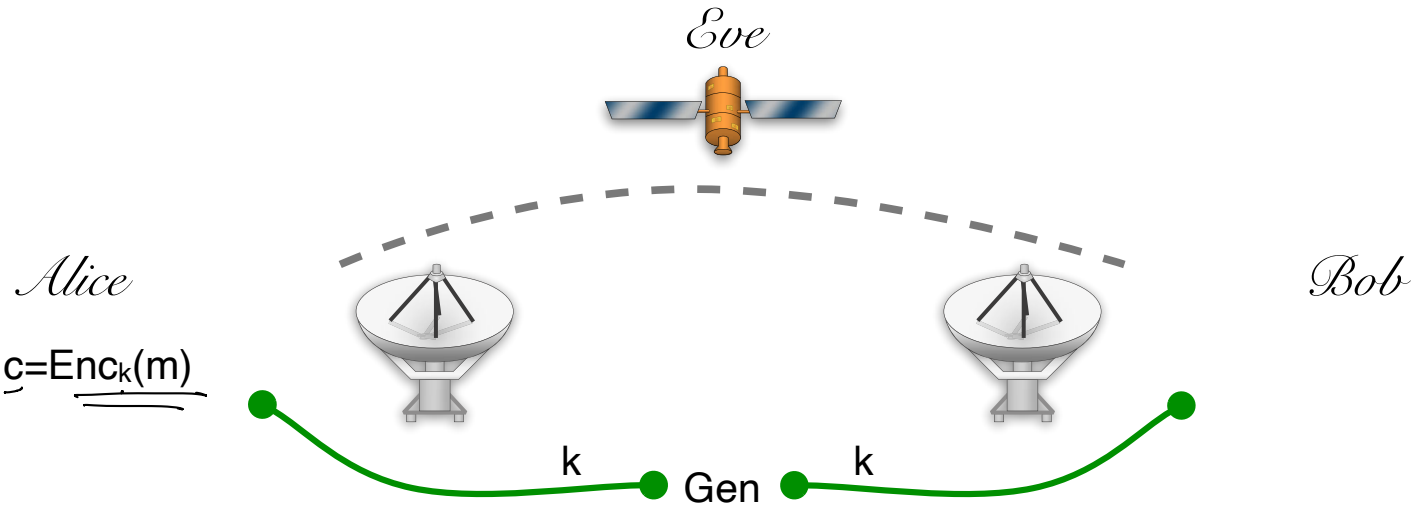
Tout le monde est d'accord pour admettre la raison d'être des

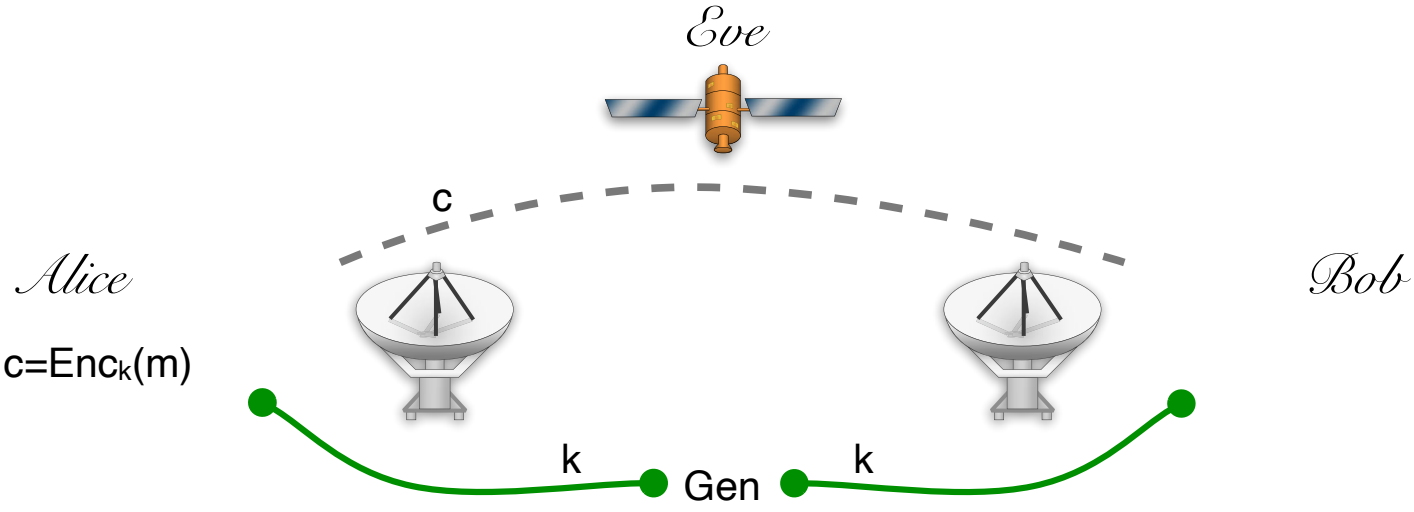
dent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

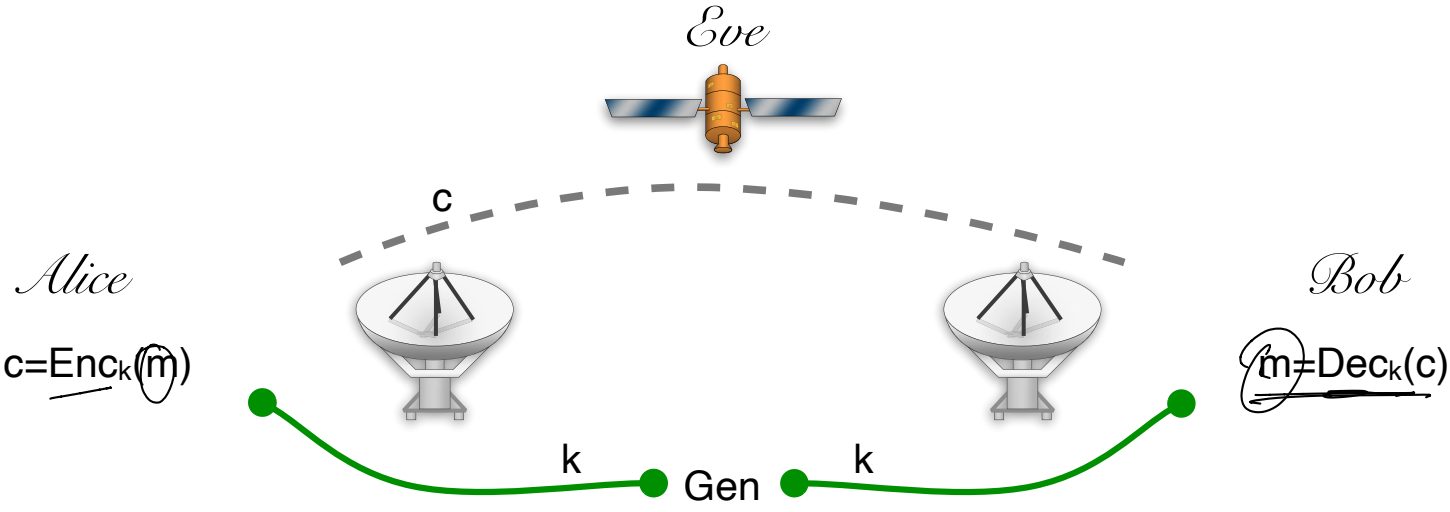
Tout le monde est d'accord pour admettre la raison d'être des

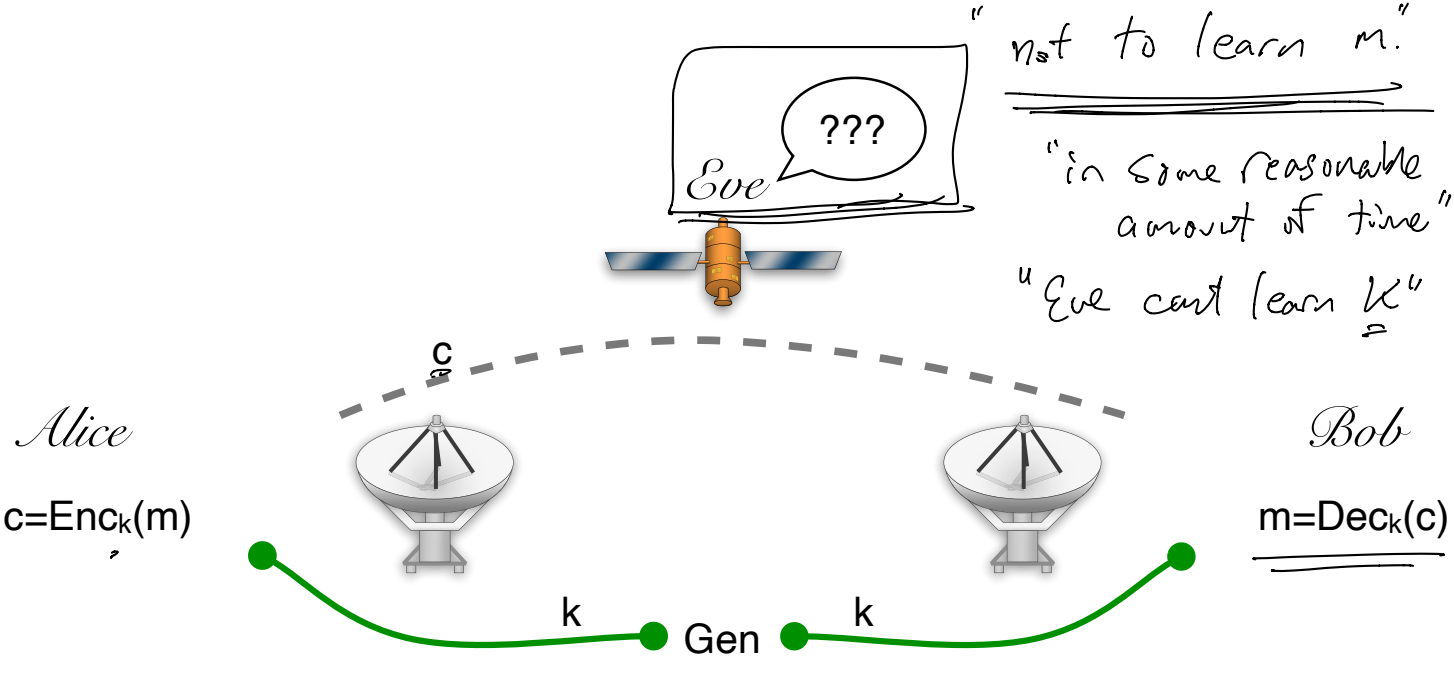

Eve
Alice
Bob


Eve
Alice
Bob
k
Gen
k


Eve
Alice
Bob
c=Enc_k(m)
k
Gen
k


Eve
c
Alice
Bob
c=Enc$_k$(m)
k
Gen
k


Eve
c
Alice
Bob
c=Enc_k(m)
m=Dec_k(c)
k
Gen
k

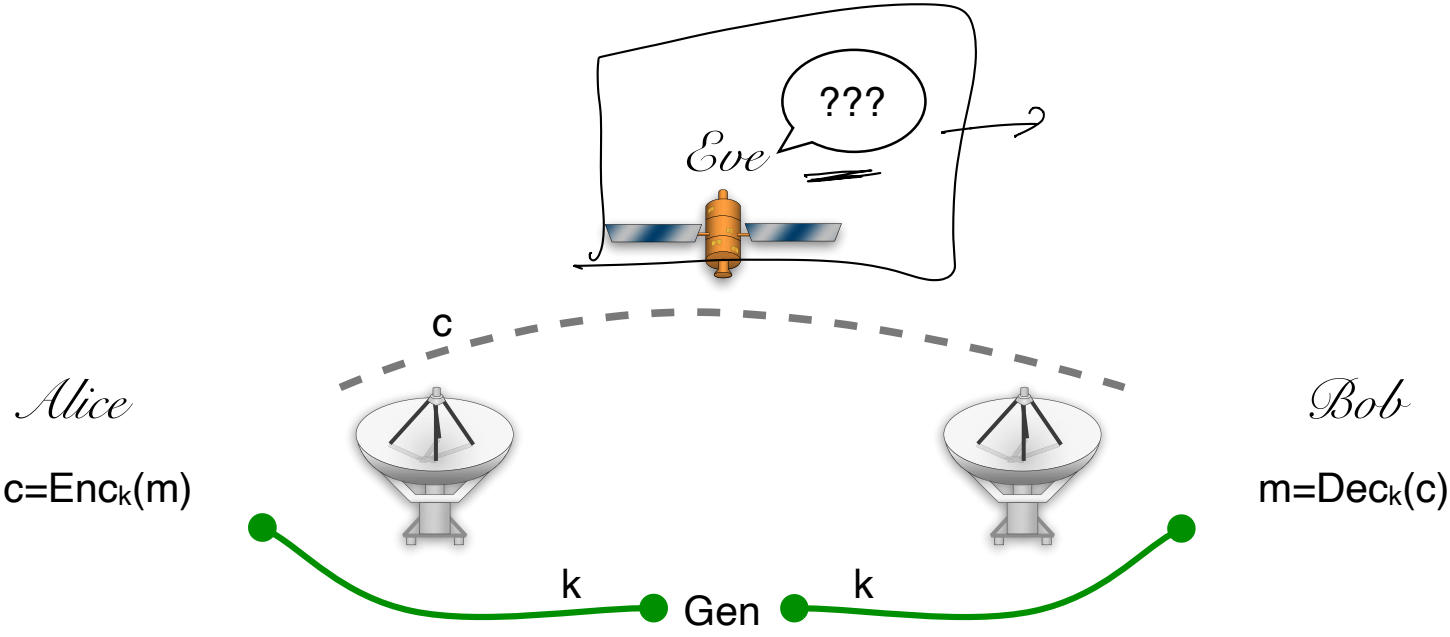


"not to learn m."

"in some reasonable amount of time"

"Eve can't learn k"

Modeling security as an experiment


???
Eve
c
Alice
Bob
c=Enc$_k$(m)
m=Dec$_k$(c)
k
Gen
k

Artwork by Bridgette Greenia

Claude Shannon.

Private key encryption

{0...2553}* messages

Keys

Gen Enc Dec

$\mathcal{M}$ $\mathcal{K}$

3 algorithms

2 sets

Private key encryption

Gen Enc Dec $\mathcal{M}$ $\mathcal{K}$

3 algorithms 2 sets

Private key encryption

Gen Enc Dec $\mathcal{M}$ $\mathcal{K}$

3 algorithms 2 sets

Gen (key generation) samples

$k \leftarrow \text{Gen s.t. } k \in \mathcal{K}$

Private key encryption

Gen Enc Dec $\mathcal{M}$ $\mathcal{K}$

3 algorithms 2 sets

Gen (key generation)

$$k \leftarrow \mathsf{Gen} \text{ s.t. } k \in \mathcal{K}$$

Enc (encryption)

$$c \leftarrow \mathsf{Enc}_k(m) \text{ for } k \in \mathcal{K}, m \in \mathcal{M}$$

Private key encryption

Gen Enc Dec $\mathcal{M}$ $\mathcal{K}$

3 algorithms 2 sets

Gen (key generation)

$k \leftarrow \mathsf{Gen}$ s.t. $k \in \mathcal{K}$

"included in"

Enc (encryption)

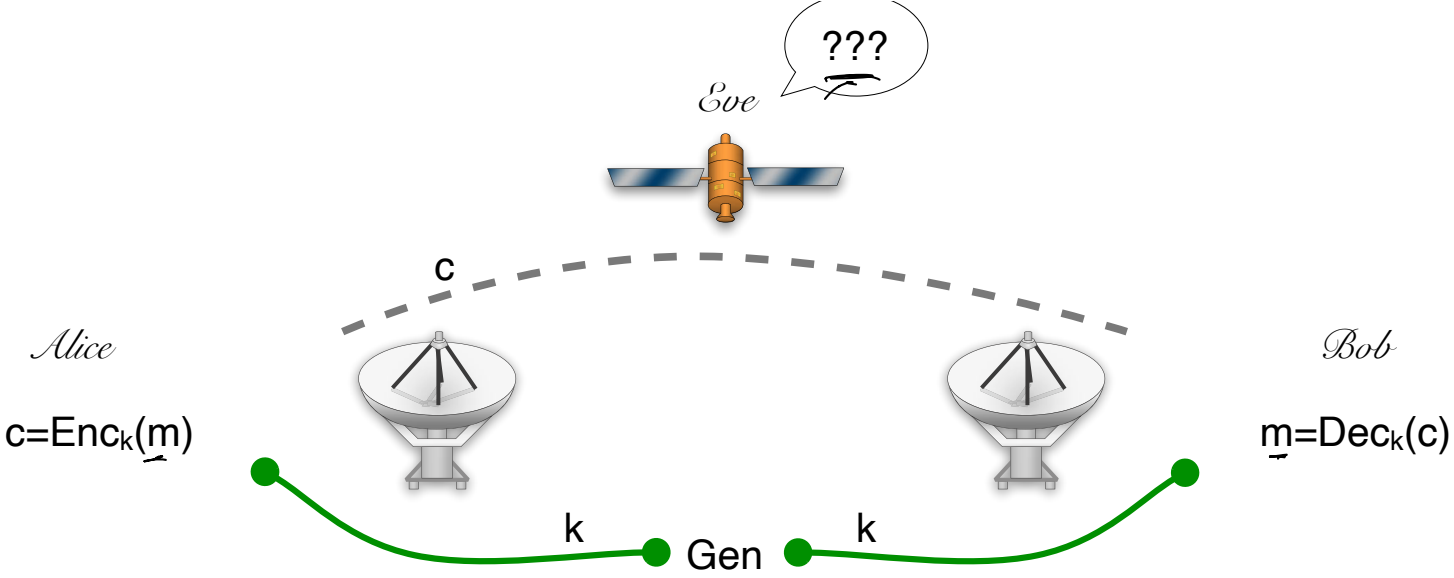
$c \leftarrow \mathsf{Enc}_k(m)$ for $k \in \mathcal{K}, m \in \mathcal{M}$

Dec (decryption)

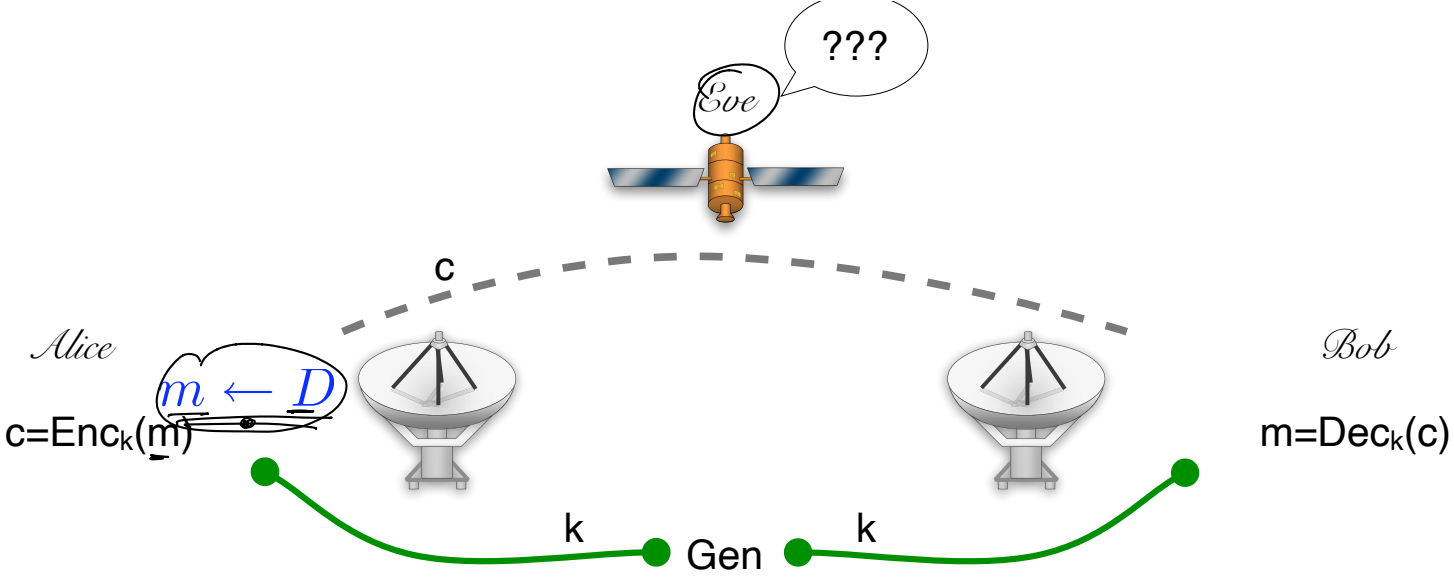
"for all" $\forall$ ∃: "there exists"

$\forall m \in \mathcal{M}, k \in \mathcal{K}$

$\Pr[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] = 1$



"Eve should not ...learn any more information about m than she knew before seeing the ciphertext c"



"Given... any apriori information about the message m, the ciphertext c does not convey any extra information"

SHANNON SECRECY

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathcal{M}, \mathcal{K})$

is said to be SHANNON-SECRET with respect to a distribution D over $\mathcal{M}$, if

what Eve already knows about the message that Alice sends to Bob.

$\forall m' \in M \; \forall c$

$$\Pr\left[m \leftarrow D \mid m' = m \right] = \Pr\left[K \leftarrow \mathsf{Gen}, m \leftarrow D \mid m' = m \text{ given } \mathsf{Enc}_K(m') = c \right]$$

Eve has about m.

"Given some a-priori information about m,
Eve cannot learn additional info about m by observing ciphertext c."

Shannon secrecy

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathcal{M}, \mathcal{K})$

is said to be SHANNON-SECRET with respect to a distribution D over $\mathcal{M}$, if

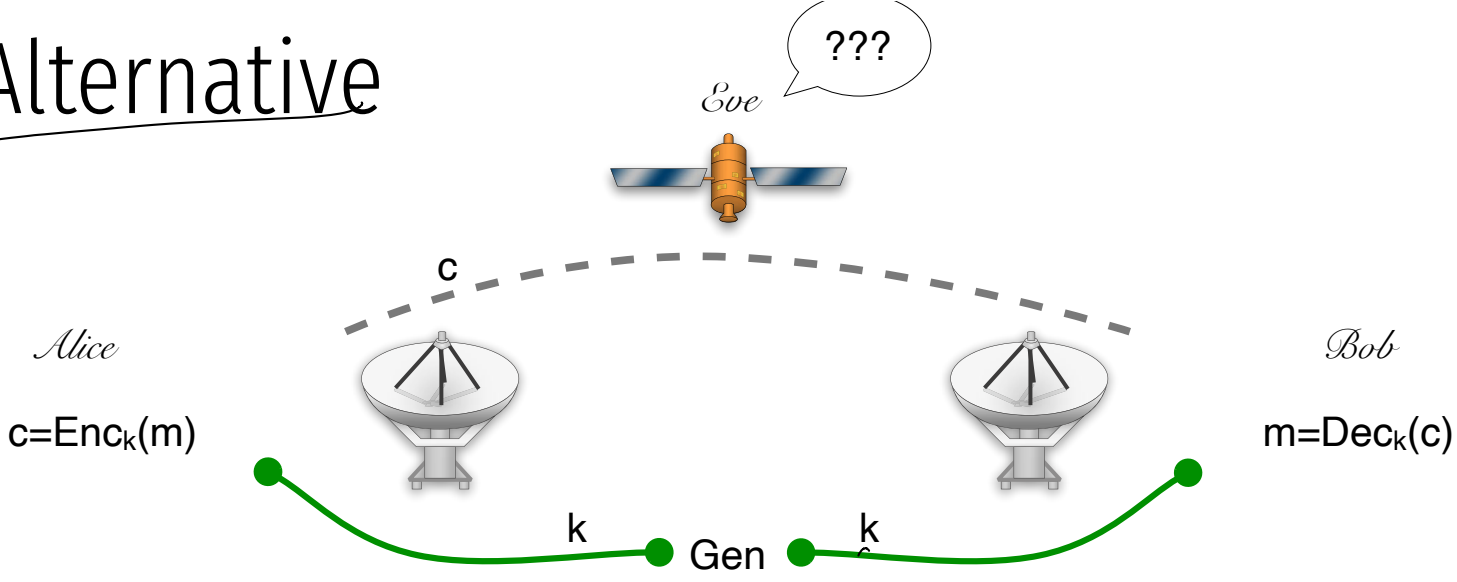
$$\forall m' \in \mathcal{M}, \forall c$$

$$\Pr[k \leftarrow \mathsf{Gen}, m \leftarrow D \ : \ m' = m \mid \mathsf{Enc}_k(m') = c]$$

$$= \Pr[m \leftarrow D \ : \ m' = m]$$

"given some a-priori information about m,
Eve cannot learn additional info about m by observing ciphertext c."

Alternative



"For any ... pair of messages $m_1, m_2 \in \mathcal{M}$
Eve cannot ... tell whether c is an "encryption of m_1 or m_2"

Perfect secrecy

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathcal{M}, \mathcal{K})$

is said to be PERFECTLY SECRET if

$$\forall m_1, m_2 \in \mathcal{M}, \forall c$$

$$\Pr[k \in \mathsf{Gen} \mid c = \mathsf{Enc}_k(m_1)] = \Pr[k \in \mathsf{Gen} \mid c = \mathsf{Enc}_k(m_2)]$$

Theorem: Perfect security ⇔ Shannon security

One-time pad (Vernam 1917)

$\oplus$ - "XOR"

		$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

AND OR

0	1
0	1
0	1
1	0

$$
\begin{aligned}
\mathcal{M} &= \{0,1\}^n \\
\mathcal{K} &= \{0,1\}^n \\
\mathsf{Gen} &= k = k_1 k_2 \ldots k_n \leftarrow \{0,1\}^n \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = m_i \oplus k_i \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = c_i \oplus k_i
\end{aligned}
$$

One-time pad is perfect.

Claim: For any c,m...

Spse I see $c = 01110010$

it could be the encryption of any message m with 8 bit

YES YES

01 0 0 10

ABC ABC

One-time pad is perfect.

Claim 13.1. *For any* $c, m \in \{0,1\}^n$*,*

$$\Pr\left[k \leftarrow \{0,1\}^n : Enc_k(m) = c\right] = 2^{-k}$$

for all c :

One-time pad is perfect.

Claim 13.1. *For any* $c, m \in \{0,1\}^n$*,*

$$\Pr\left[k \leftarrow \{0,1\}^n : Enc_k(m) = c\right] = 2^{-k}$$

Claim 13.2. *For any* $c \notin \{0,1\}^n, m \in \{0,1\}^n$*,*

$$\Pr\left[k \leftarrow \{0,1\}^n : Enc_k(m) = c\right] = 0$$

for all c :

One-time pad is perfect.

Claim 13.1. *For any* $c, m \in \{0,1\}^n$*,*

$$\Pr\left[k \leftarrow \{0,1\}^n : Enc_k(m) = c\right] = 2^{-k}$$

Claim 13.2. *For any* $c \notin \{0,1\}^n, m \in \{0,1\}^n$*,*

$$\Pr\left[k \leftarrow \{0,1\}^n : Enc_k(m) = c\right] = 0$$

for all c :

$$\Pr_k[\mathsf{Enc}_k(m_1) = c] = \Pr_k[\mathsf{Enc}_k(m_2) = c]$$

q.e.d.

One-time pad

ANY PROBLEMS?

$$
\begin{aligned}
\mathcal{M} &= \{0,1\}^n \\
\mathcal{K} &= \{0,1\}^n \\
\mathsf{Gen} &= k = k_1 k_2 \ldots k_n \leftarrow \{0,1\}^n \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = m_i \oplus k_i \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = c_i \oplus k_i
\end{aligned}
$$