2550 Intro to cybersecurity

L2

abhi shelat

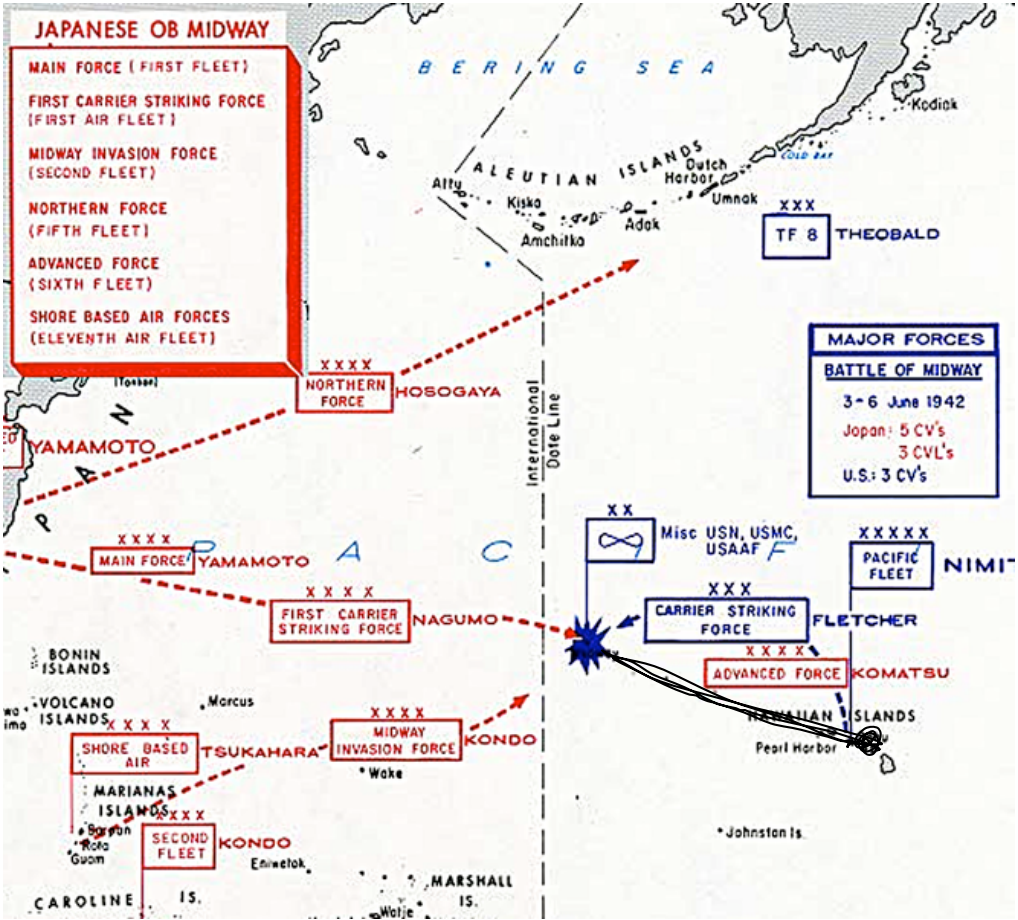
What does it mean to attack a system?

Violation of Expectations

What are our expectations?

Correctness, Responsiveness,

- Confidentiality
- Integrity
- Authenticity
- Non-repudiation


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
International Date Line
YAMAMOTO
XXXX
MAIN FORCE
YAMAMOTO
XX
Misc USN, USMC, USAAF
XXXXX
PACIFIC FLEET
NIMI
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
Pearl Harbor
MARIANAS ISLANDS
XXX
SECOND FLEET
KONDO
Saipan
Rota
Guam
Eniwetok
Johnston Is.
CAROLINE IS.
MARSHALL IS.
Wotje

"AF"

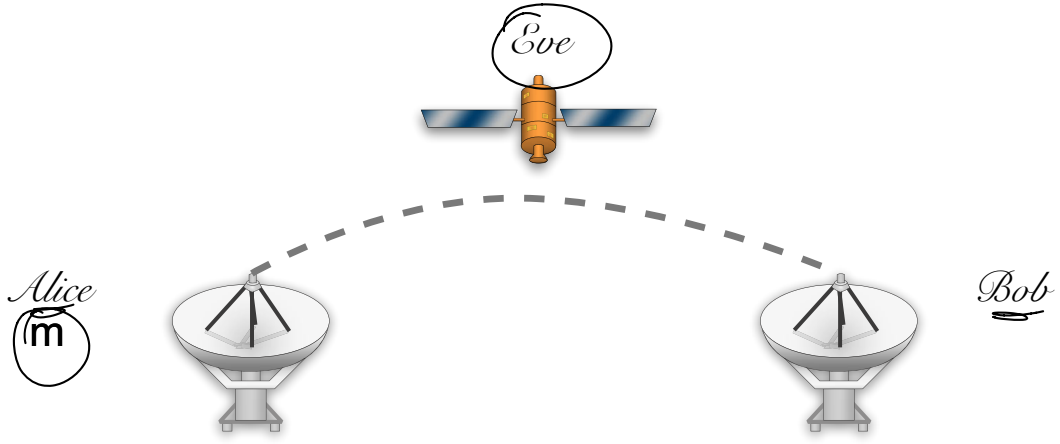
june 1942

jn-25b

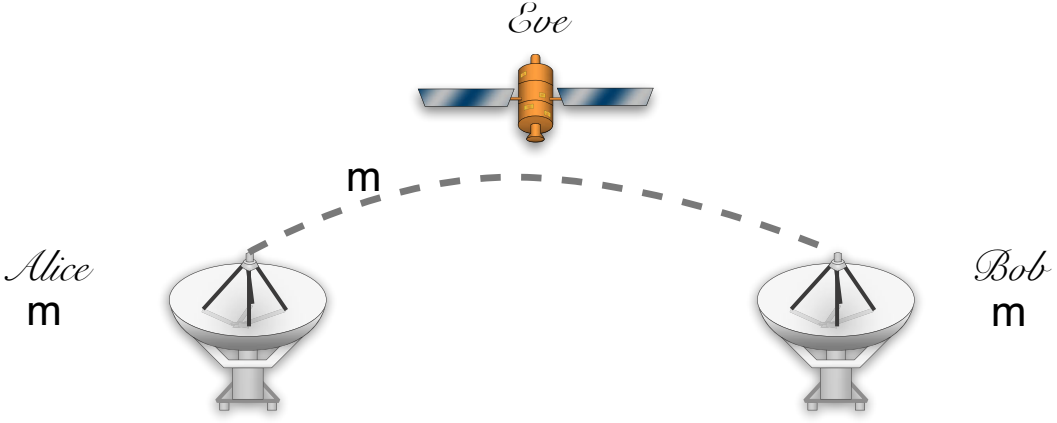
CMDR EDWARD T LAYTON
(FLEET INTELLIGENCE OFFICER)

LT CMDR JOSEPH ROCHEFORT
(COMBAT INTELLIGENCE UNIT)

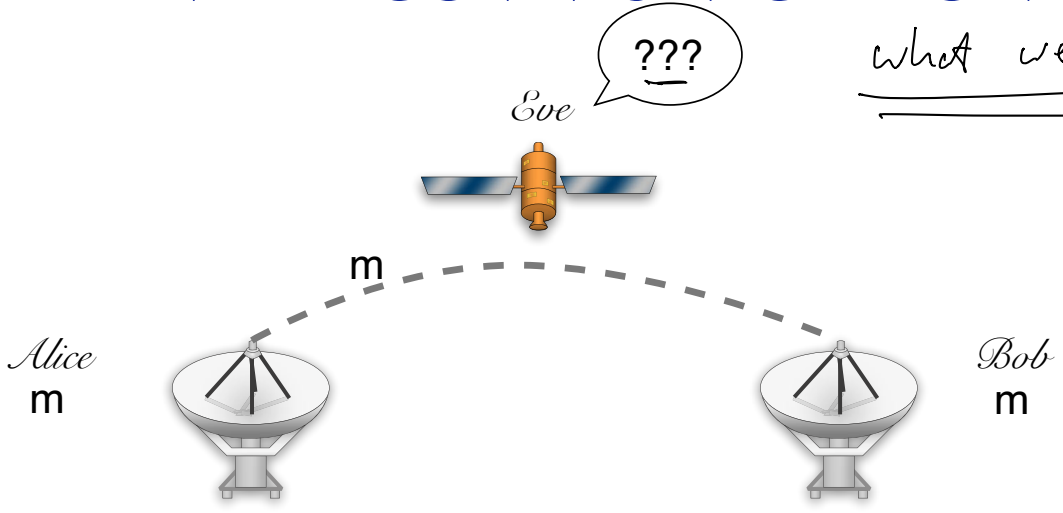
PRIVATE COMMUNICATION



PRIVATE COMMUNICATION



PRIVATE COMMUNICATION

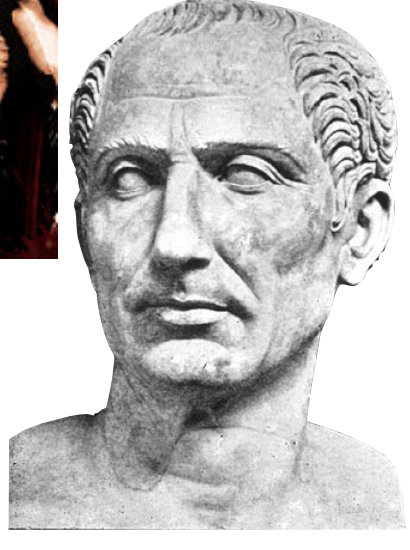


what we want

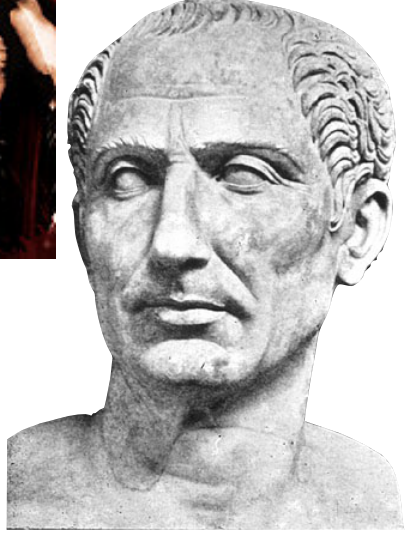
Abstraction of the problem.


WIDESCREEN EDITION
300

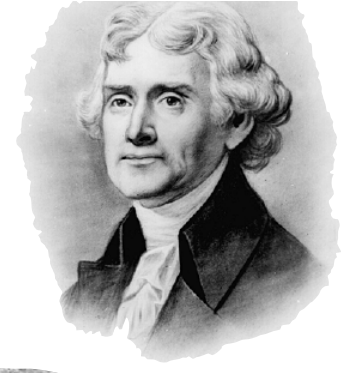

WIDESCREEN EDITION
300

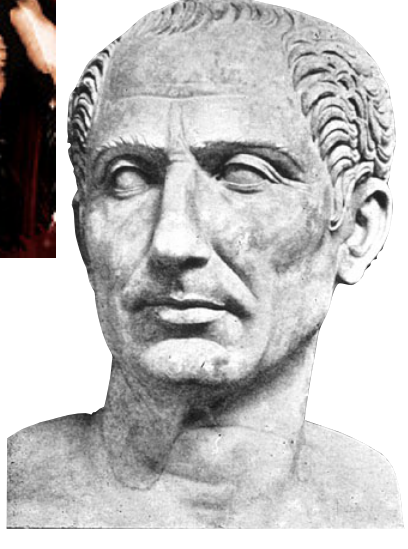



WIDESCREEN EDITION
300

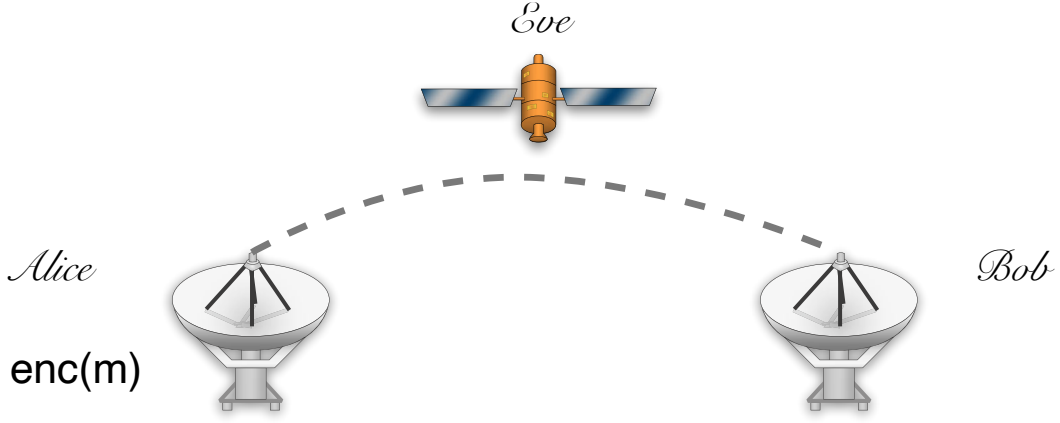



WIDESCREEN EDITION
300

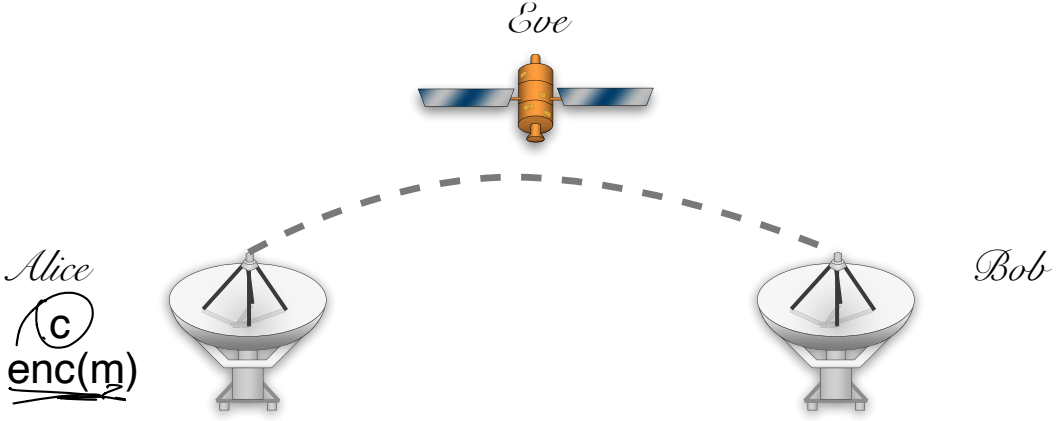




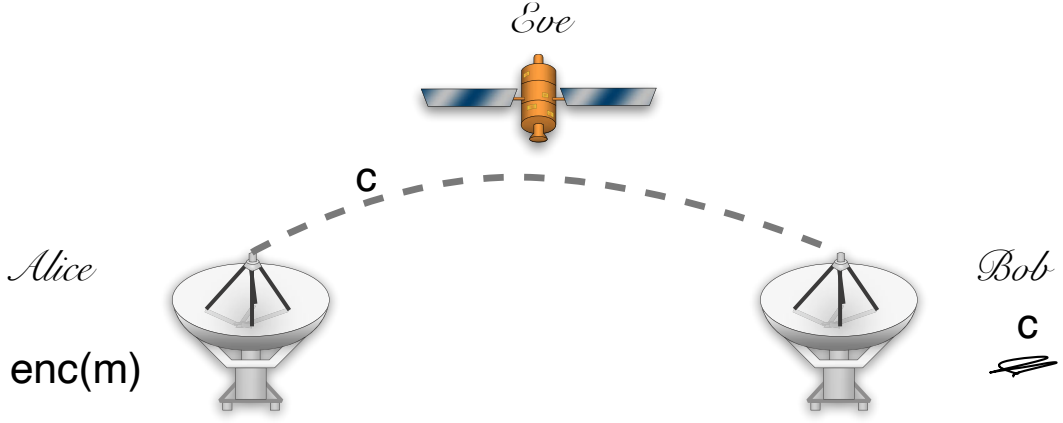
PRIVATE



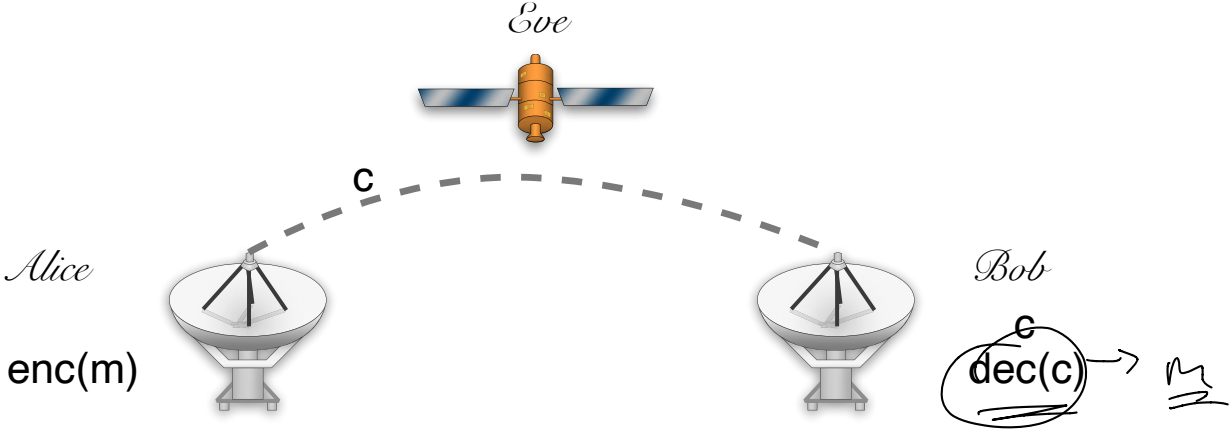
PRIVATE



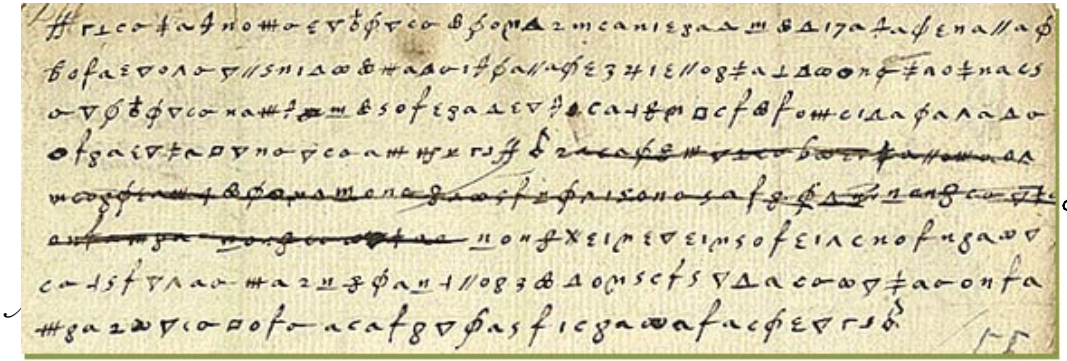
PRIVATE

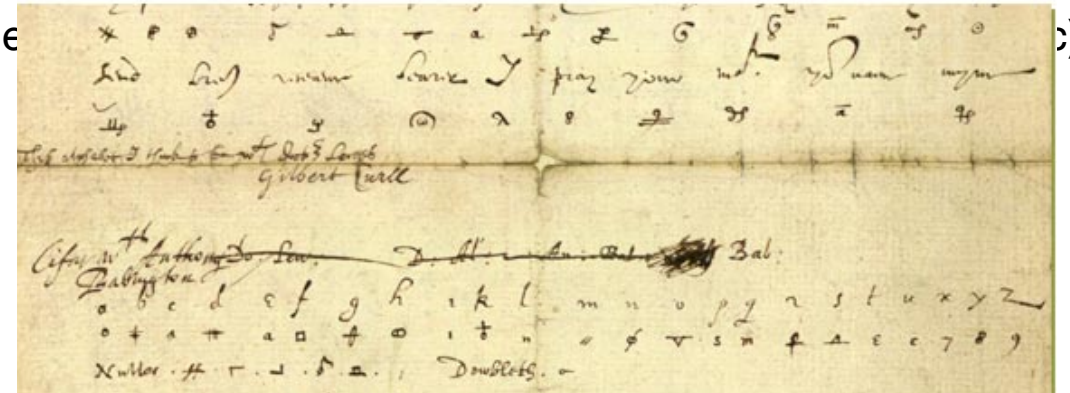


PRIVATE



PRIVATE





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

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

MINIMIZE THE ASSUMPTIONS ON WHICH THE SYSTEM RELIES

Abstraction

Operation

Implementation —

Design

Abstraction

Implementation

Design

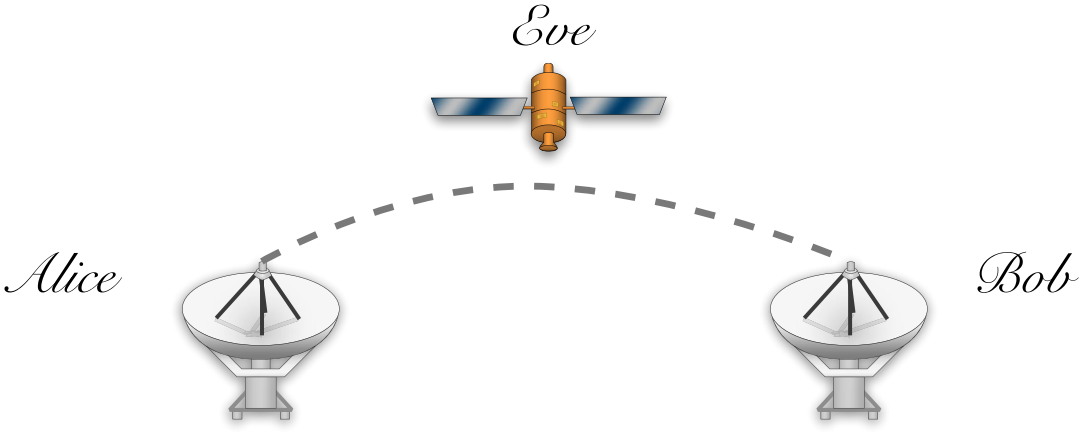
Abstraction

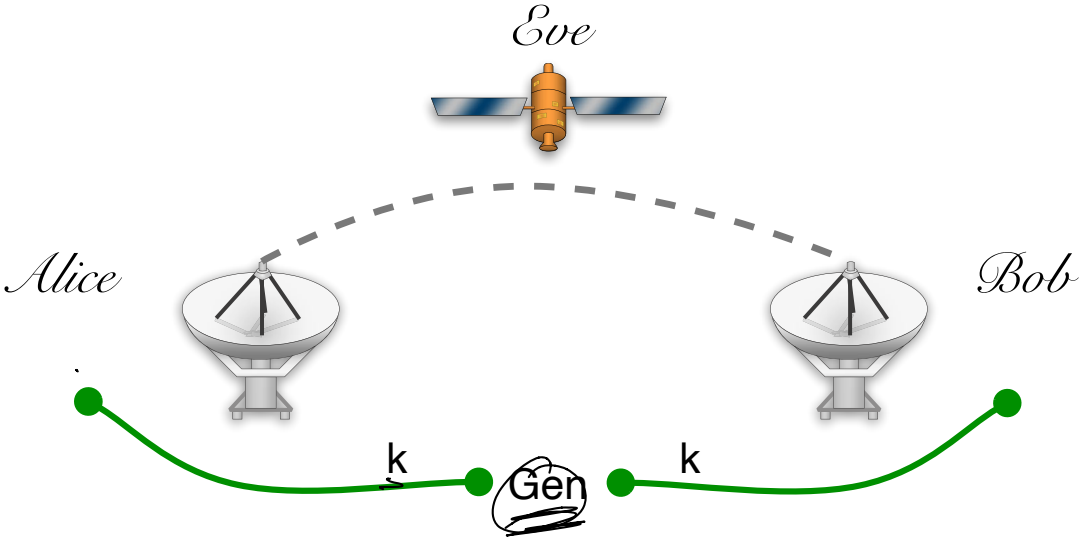
Usage

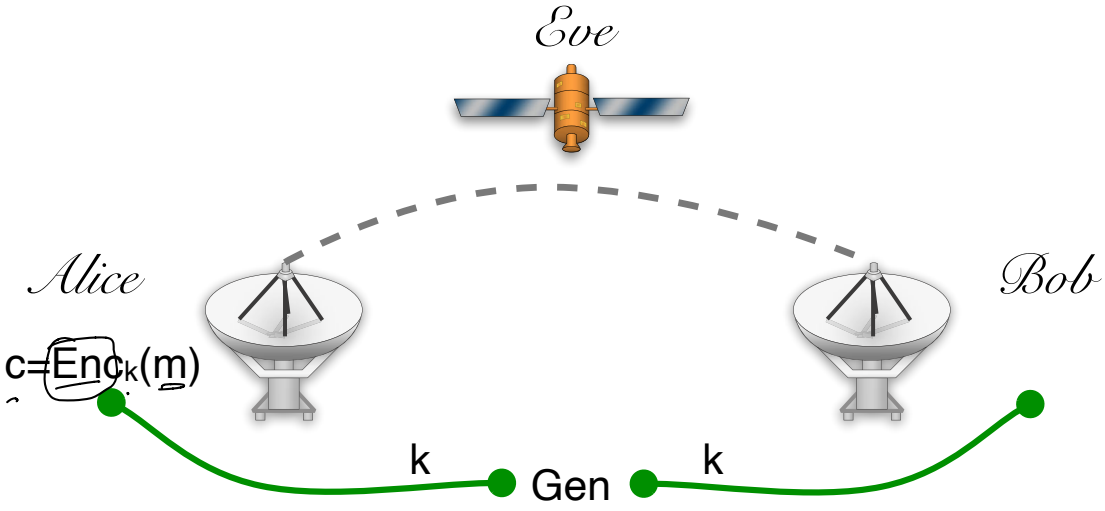
Implementation

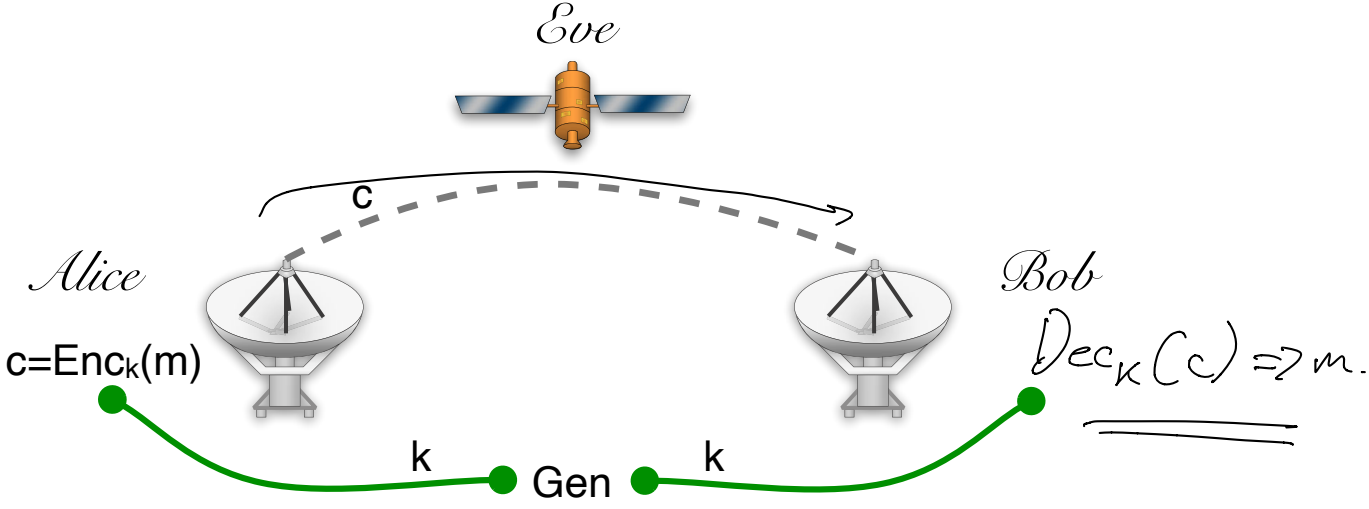
Design

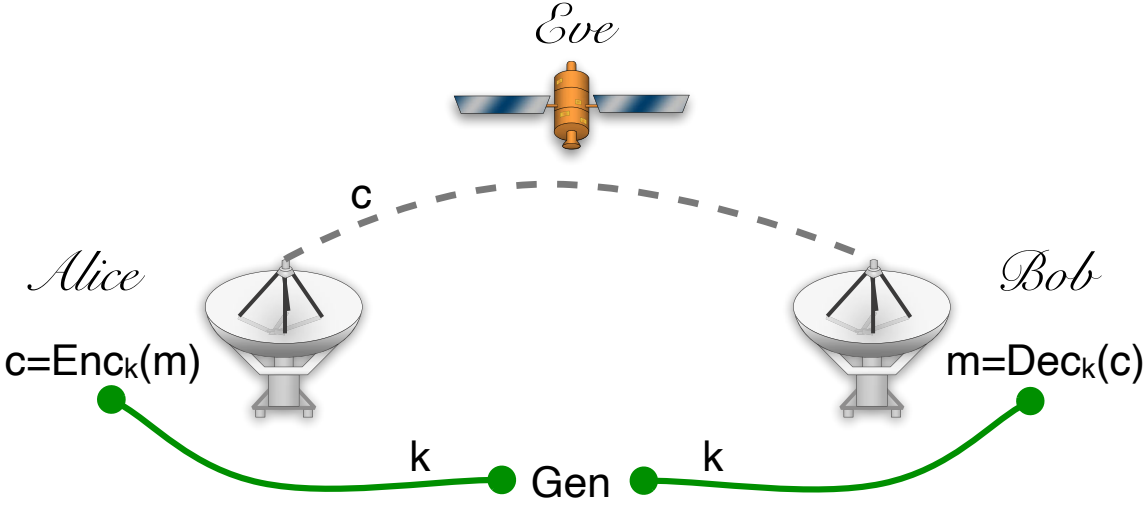
Abstraction

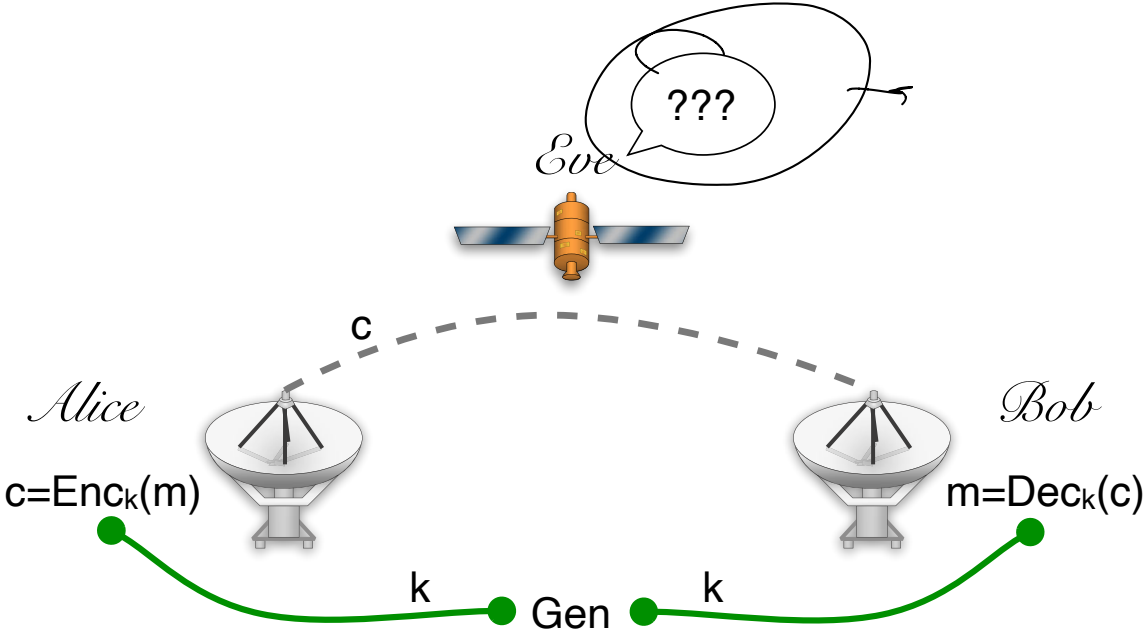

Eve
Alice
Bob


Eve
Alice
Bob
k
Gen
k


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


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


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


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

Caesar Cipher

$$
\begin{aligned}
\mathcal{M} &= \{A, B, \ldots, Z\}^* \\
\mathcal{K} &= \{0, 1, 2, \ldots, 25\} \\
\mathsf{Gen} &= k \text{ where } k \xleftarrow{r} \mathcal{K}. \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = m_i + k \bmod 26 \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = c_i - k \bmod 26
\end{aligned}
$$

WKH PRGHUQ VWXGB RI FUBSWRJUDSKB LQYHVWLJDWHV WHFKQLTXHV IRU
IDFLOLWDWLQJ LQWHUDFWLRQV EHWZHHQ GLVWUXVWIXO HQWLWLHV LQ RXU
FRQQHFWHG VRFLHWB VXFK WHFKQLTXHV KDYH EHFRPH LQGLVSHQVDEOH HQDEOLQJ
IRU LQVWDQFH DXWRPDWHG WHOOHU PDFKLQHV VHFXUH ZLUHOHVV QHWZRUNV
LQWHUQHW EDQNLQJ VDWHOOLWH UDGLRWHOHYLVLRQ DQG PRUH LQ WKLV FRXUVH ZH
LQWURGXFH VRPH RI WKH IXQGDPHQWDO FRQFHSWV RI WKLV VWXGB HPSKDVLV ZLOO
EH SODFHG RQ ULJRURXV SURRIV RI VHFXULWB EDVHG RQ SUHFLVH GHILQLWLRQV
DQG DVVXPSWLRQV

WKH PRGHUQ VWXGB RI FUBSWRJUDSKB LQYHVWLJDWHV WHFKQLTXHV IRU
IDFLOLWDWLQJ LQWHUDFWLRQV EHWZHHQ GLVWUXVWIXO HQWLWLHV LQ RXU
FRQQHFWHG VRFLHWB VXFK WHFKQLTXHV KDYH EHFRPH LQGLVSHQVDEOH HQDEOLQJ
IRU LQVWDQFH DXWRPDWHG WHOOHU PDFKLQHV VHFXUH ZLUHOHVV QHWZRUNV
LQWHUQHW EDQNLQJ VDWHOOLWH UDGLRWHOHYLVLRQ DQG PRUH LQ WKLV FRXUVH ZH
LQWURGXFH VRPH RI WKH IXQGDPHQWDO FRQFHSWV RI WKLV VWXGB HPSKDVLV ZLOO
EH SODFHG RQ ULJRURXV SURRIV RI VHFXULWB EDVHG RQ SUHFLVH GHILQLWLRQV
DQG DVVXPSWLRQV

k=1 VJG OQFGTP UVWFA QH ETARVQITCRJA KPXGUVKICVGU VGEJPKSWGU HQT HC

WKH PRGHUQ VWXGB RI FUBSWRJUDSKB LQYHVWLJDWHV WHFKQLTXHV IRU
IDFLOLWDWLQJ LQWHUDFWLRQV EHWZHHQ GLVWUXVWIXO HQWLWLHV LQ RXU
FRQQHFWHG VRFLHWB VXFK WHFKQLTXHV KDYH EHFRPH LQGLVSHQVDEOH HQDEOLQJ
IRU LQVWDQFH DXWRPDWHG WHOOHU PDFKLQHV VHFXUH ZLUHOHVV QHWZRUNV
LQWHUQHW EDQNLQJ VDWHOOLWH UDGLRWHOHYLVLRQ DQG PRUH LQ WKLV FRXUVH ZH
LQWURGXFH VRPH RI WKH IXQGDPHQWDO FRQFHSWV RI WKLV VWXGB HPSKDVLV ZLOO
EH SODFHG RQ ULJRURXV SURRIV RI VHFXULWB EDVHG RQ SUHFLVH GHILQLWLRQV
DQG DVVXPSWLRQV

k=1 VJG OQFGTP UVWFA QH ETARVQITCRJA KPXGUVKICVGU VGEJPKSWGU HQT HC

k=2 UIF NPEFSO TUVEZ PG DSZQUPHSBQIZ JOWFTUJHBUFT UFDIOJRVFT GPS GB

WKH PRGHUQ VWXGB RI FUBSWRJUDSKB LQYHVWLJDWHV WHFKQLTXHV IRU
IDFLOLWDWLQJ LQWHUDFWLRQV EHWZHHQ GLVWUXVWIXO HQWLWLHV LQ RXU
FRQQHFWHG VRFLHWB VXFK WHFKQLTXHV KDYH EHFRPH LQGLVSHQVDEOH HQDEOLQJ
IRU LQVWDQFH DXWRPDWHG WHOOHU PDFKLQHV VHFXUH ZLUHOHVV QHWZRUNV
LQWHUQHW EDQNLQJ VDWHOOLWH UDGLRWHOHYLVLRQ DQG PRUH LQ WKLV FRXUVH ZH
LQWURGXFH VRPH RI WKH IXQGDPHQWDO FRQFHSWV RI WKLV VWXGB HPSKDVLV ZLOO
EH SODFHG RQ ULJRURXV SURRIV RI VHFXULWB EDVHG RQ SUHFLVH GHILQLWLRQV
DQG DVVXPSWLRQV

k=1 VJG OQFGTP UVWFA QH ETARVQITCRJA KPXGUVKICVGU VGEJPKSWGU HQT HC

k=2 UIF NPEFSO TUVEZ PG DSZQUPHSBQIZ JOWFTUJHBUFT UFDIOJRVFT GPS GB

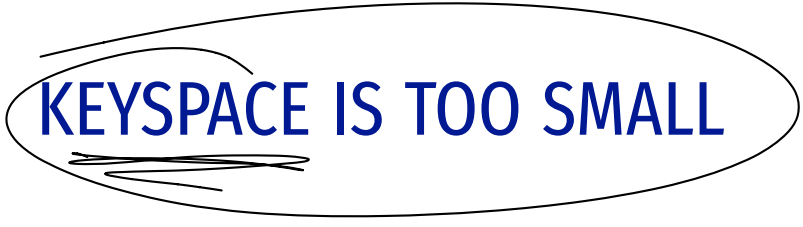
k=3 THE MODERN STUDY OF CRYPTOGRAPHY INVESTIGATES TECHNIQUES FOR FA

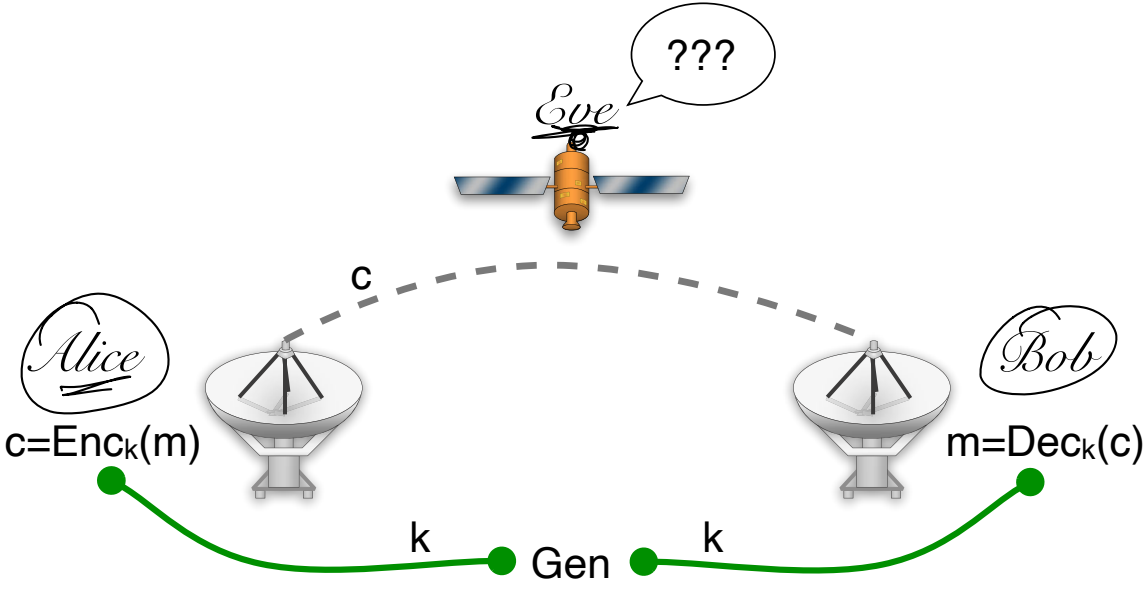
WKH PRGHUQ VWXGB RI FUBSWRJUDSKB LQYHVWLJDWHV WHFKQLTXHV IRU
IDFLOLWDWLQJ LQWHUDFWLRQV EHWZHHQ GLVWUXVWIXO HQWLWLHV LQ RXU
FRQQHFWHG VRFLHWB VXFK WHFKQLTXHV KDYH EHFRPH LQGLVSHQVDEOH HQDEOLQJ
IRU LQVWDQFH DXWRPDWHG WHOOHU PDFKLQHV VHFXUH ZLUHOHVV QHWZRUNV
LQWHUQHW EDQNLQJ VDWHOOLWH UDGLRWHOHYLVLRQ DQG PRUH LQ WKLV FRXUVH ZH
LQWURGXFH VRPH RI WKH IXQGDPHQWDO FRQFHSWV RI WKLV VWXGB HPSKDVLV ZLOO
EH SODFHG RQ ULJRURXV SURRIV RI VHFXULWB EDVHG RQ SUHFLVH GHILQLWLRQV
DQG DVVXPSWLRQV

k=1 VJG OQFGTP UVWFA QH ETARVQITCRJA KPXGUVKICVGU VGEJPKSWGU HQT HC

k=2 UIF NPEFSO TUVEZ PG DSZQUPHSBQIZ JOWFTUJHBUFT UFDIOJRVFT GPS GB

k=3 THE MODERN STUDY OF CRYPTOGRAPHY INVESTIGATES TECHNIQUES FOR FA




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

Abstraction

Design

Abstraction

Implementation

Design

Abstraction

Usage

Implementation

Design

Abstraction

Substitution cipher

k = CATSRFUNDEG...Z

A B C D E F G H I

$$
\begin{array}{rcl}
\mathcal{M} & = & \{A, B, \ldots, Z\}^* \\
\mathcal{K} & = & \text{the set of permutations over } \{A, B, \ldots, Z\} \\
\mathsf{Gen} & = & k \text{ where } k \xleftarrow{r} \mathcal{K}. \\
Enc_k(m_1 m_2 \ldots m_n) & = & c_1 c_2 \ldots c_n \text{ where } c_i = k(m_i) \\
Dec_k(c_1 c_2 \ldots c_n) & = & m_1 m_2 \ldots m_n \text{ where } m_i = k^{-1}(c_i)
\end{array}
$$

ABHI ~ CAND

Substitution cipher

$$
\begin{aligned}
\mathcal{M} &= \{A, B, \ldots, Z\}^* \\
\mathcal{K} &= \text{the set of permutations over } \{A, B, \ldots, Z\} \\
\mathsf{Gen} &= k \text{ where } k \xleftarrow{r} \mathcal{K}. \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = k(m_i) \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = k^{-1}(c_i)
\end{aligned}
$$

size of keyspace is

$26! = 403291461126605635584000000$

EOR TZSRWF XEASG ZV DWGYEZPWQYOG NFKRXENPQERX ERDOFNIARX VZW
VQDNHNEQENFP NFERWQDENZFX UREJRRF SNXEWAXEVAH RFENENRX NF ZAW
DZFFRDERS XZDNREG XADO ERDOFNIARX OQKR URDZTR NFSNXYRFXQUHR RFQUHNFP
VZW NFXEQFDR QAEZTQERS ERHHRW TQDONFRX XRDAWR JNWRHRXX FREJZWLX
NFERWFRE UQFLNFP XQERHHNER WQSNZERHRKNXNZF QFS TZWR NF EONX DZAWXR
JR NFEWZSADR XZTR ZV EOR VAFSQTRFEQH DZFDRYEX ZV EONX XEASG RTYOQXNX
JNHH UR YHQDRS ZF WNPZWZAX YWZZVX ZV XRDAWNEG UQXRS ZF YWRDNXR
SRVNFNENZFX QFS QXXATYENZFX

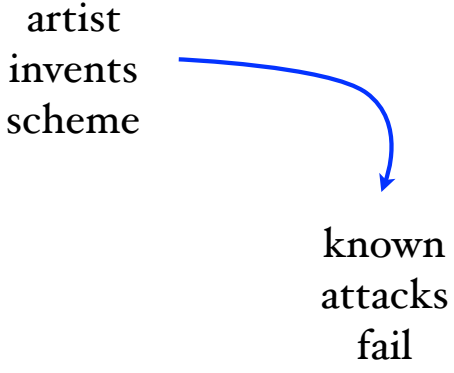
EOR TZSRWF XEASG ZV DWGYEZPWQYOG NFKRXENPQERX ERDOFNIARX VZW
VQDNHNEQENFP NFERWQDENZFX UREJRRF SNXEWAXEVAH RFENENRX NF ZAW
DZFFRDERS XZDNREG XADO ERDOFNIARX OQKR URDZTR NFSNXYRFXQUHR RFQUHNFP
VZW NFXEQFDR QAEZTQERS ERHHRW TQDONFRX XRDAWR JNWRHRXX FREJZWLX
NFERWFRE UQFLNFP XQERHHNER WQSNZERHRKNXNZF QFS TZWR NF EONX DZAWXR
JR NFEWZSADR XZTR ZV EOR VAFSQTRFEQH DZFDRYEX ZV EONX XEASG RTYOQXNX
JNHH UR YHQDRS ZF WNPZWZAX YWZZVX ZV XRDAWNEG UQXRS ZF YWRDNXR
SRVNFNENZFX QFS QXXATYENZFX

FREQUENCY ANALYSIS

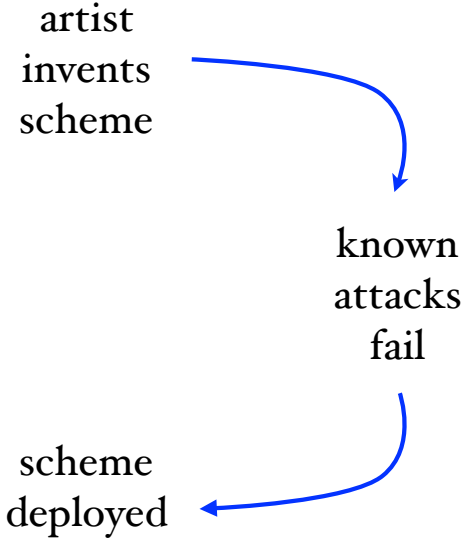
classic crypto cycle

artist
invents
scheme

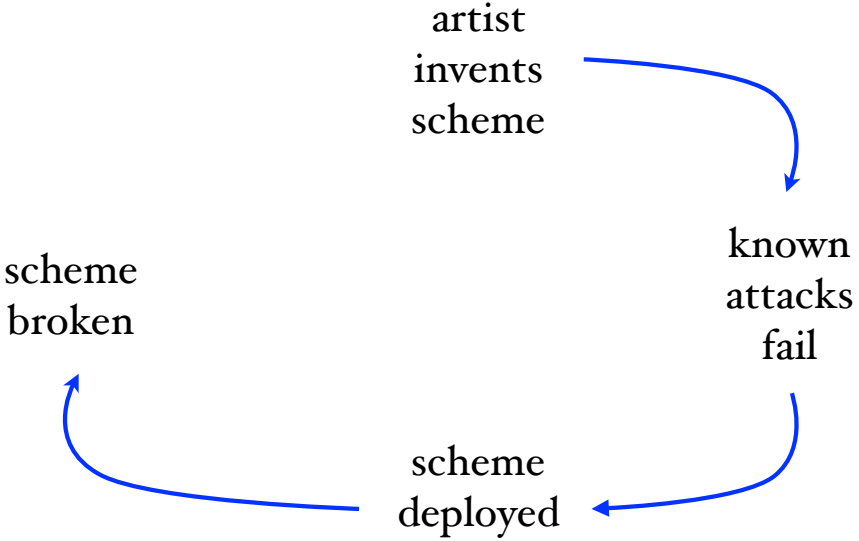
classic crypto cycle



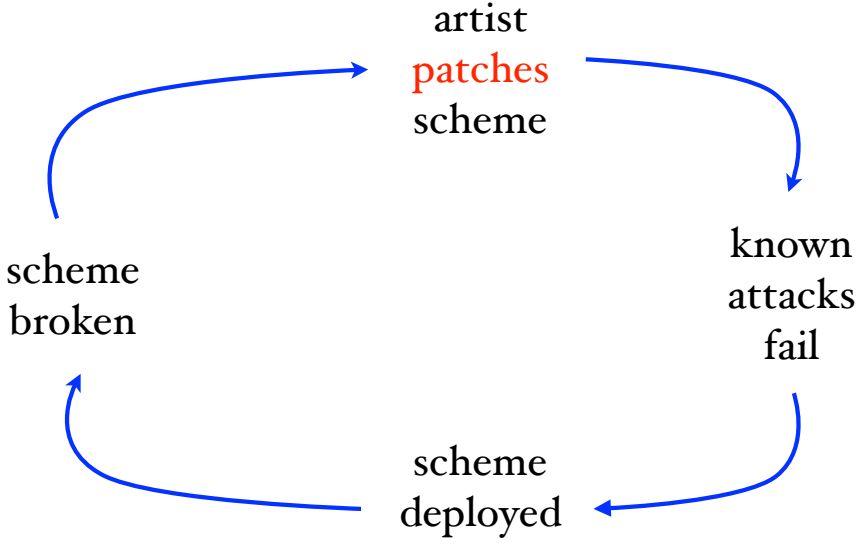
classic crypto cycle



classic crypto cycle



classic crypto cycle



modern cryptography

formulate mathematical definitions

formulate precise mathematical assumptions
"factoring is hard"

provide a proof of security:
prove: if scheme can be
broken, assumption is false.

modern cryptography

formulate mathematical definitions

formulate precise mathematical assumptions

provide a proof of security.

160841390303024853461857069924181865202614121764998031571894360060933576495286036488414622134387194956133542423727184181 3

"factoring is hard"

prove: if scheme can be broken, assumption is false.

modern cryptography

formulate mathematical definitions

formulate precise mathematical assumptions
"factoring is hard"

provide a proof of security:
prove: if scheme can be
broken, assumption is false.