Cryptography (5830)

Computational indistinguishability
Stream ciphers, block ciphers
Reduction-based approach to analysis

Towards computational indistinguishability

Def. A symmetric encryption scheme is perfectly secure if for all messages M,M' and ciphertexts C

$$\Pr[\,\mathrm{Enc}(K,M) = C\,] = \Pr[\,\mathrm{Enc}(K,M') = C\,]$$

where probabilities are over choice of K

Let's give a game-based formulation of this using an adversary
Let SE = (Kg,Enc,Dec) be a symmetric encryption scheme
Let $\mathcal{A}$ Let be a randomized algorithm, called the adversary

IND(SE,$\mathcal{A}$):
(st,M_0,M_1) <-$ $\mathcal{A}_1$
K <-$ Kg ; b <-$ {0,1}
C <-$ Enc(K,M_b)
b' <-$ $\mathcal{A}_2$ (st, C)
Return (b = b')

IND(SE,$\mathcal{A}$)'s output is 1 if (b = b').
We say then that the adversary succeeded

Def. A scheme SE is perfectly secure if for every $\mathcal{A}$ it is the case that

$$\Pr[\mathrm{IND}(SE,\mathcal{A}) = 1] = 1/2$$

Computational indistinguishability

Def. A symmetric encryption scheme is (t, ϵ)-indistinguishable if for any adversary $\mathcal{A}$ running in time at most t it holds that

$$\Pr[\text{IND}(\text{SE}, \mathcal{A}) = 1] \leq 1/2 + \epsilon$$

1) Tiny adversarial success

2) Computationally limited adversary

Discussion questions:

1) Does (t, ϵ)-indistinguishability model known, chosen message attack? What about chosen ciphertext?
2) Is a OTP (t, ϵ)-indistinguishable?
3) Is a substitution cipher (t, ϵ)-indistinguishable?

How do we build computationally-secure SE schemes?

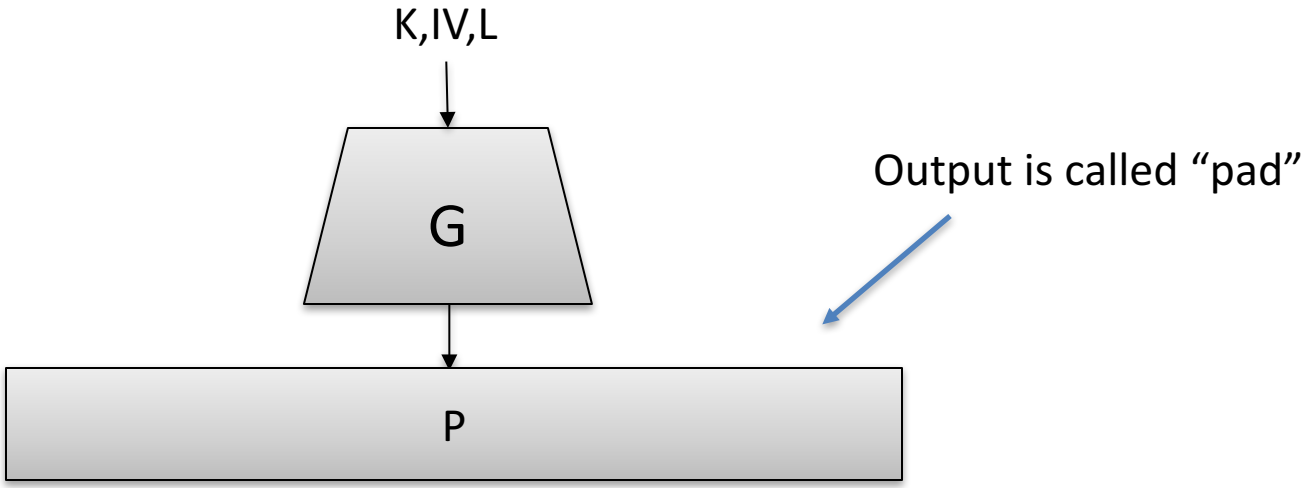
We will take a reductionist approach

- Introduce stream ciphers, build encryption from it
- Introduce block ciphers
- Build stream ciphers from block ciphers
- Prove that block cipher security implies indistinguishability

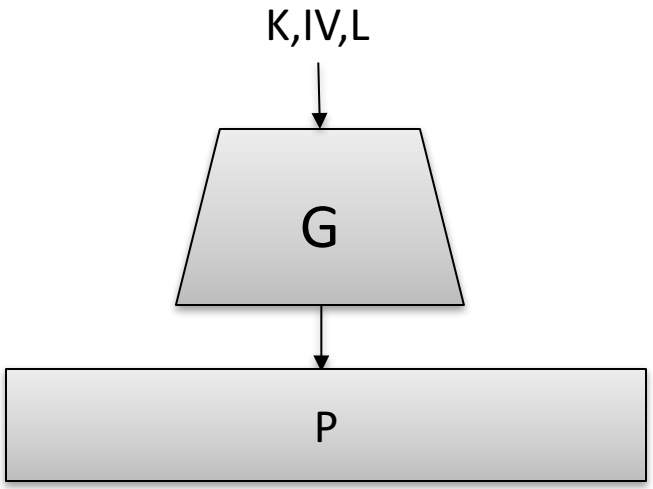
Stream ciphers

A stream cipher is a pair of algorithms (Kg,G):

- Kg outputs a random key K
- G(K,IV) takes secret K, additional random value IV (called initialization vector, can be public), desired length L, outputs string P with |P| = L



Stream cipher security



(t, ϵ)-pseudorandom generator: no attacker limited to time t can distinguish between IV,G(K,IV,L) and random bitstring of length L with advantage greater ϵ

PRG(G,L,$\mathcal{B}$):
K <-$ Kg ; IV <-$ $\{0,1\}^n$
P_1 <- G(K,IV,L)
P_0 <- $\{0,1\}^L$
b <-$ {0,1}
b' <-$ $\mathcal{B}$ (IV, P_b)
Return (b = b')

Advantage:

ϵ = | Pr[PRG1(G,L,$\mathcal{B}$) = 1] - Pr[PRG0(G,L,$\mathcal{B}$) = 0] |

PRG game with b fixed to 1

PRG game with b fixed to 0

SE from a stream cipher

Say we have a secure stream cipher. How do we build an SE scheme?

Kg():
$K \xleftarrow{\$} \{0,1\}^k$

Pick a random key

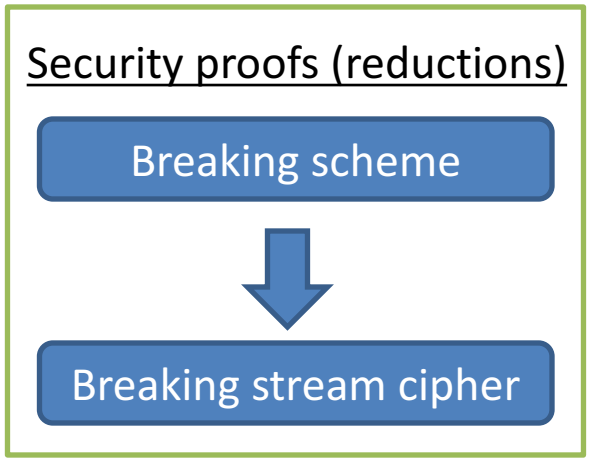
Enc(K,M):
$L \leftarrow |M|$
$IV \xleftarrow{\$} \{0,1\}^n$
Return $(IV, G(K,IV,L) \oplus M)$

Dec(K,(IV,C)):
$L \leftarrow |C|$
Return $G(K,IV,L) \oplus C$

Assume ciphertext can be parsed into IV and remaining ciphertext bits

Reduction-based security analysis

Goal: show that if stream cipher is secure, then encryption is secure



Attacker $\mathcal{A}$ violates
(t, ϵ)-indistinguishability security

For any $\mathcal{A}$ need to give $\mathcal{B}$ for which $t' \approx t$ and $\epsilon' \approx \epsilon$

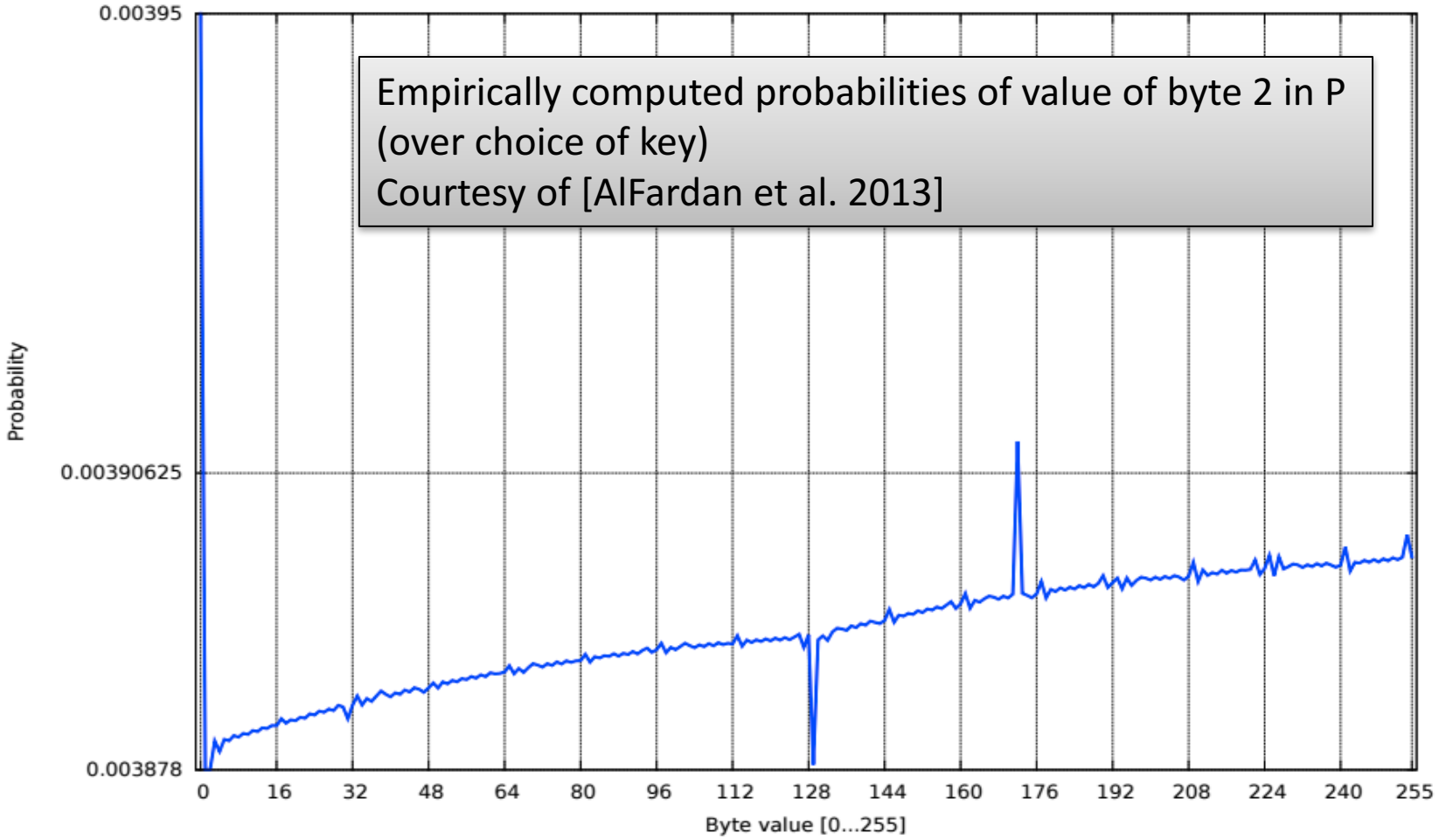
Attacker $\mathcal{B}$ violates
(t', ϵ')-pseudorandom generator security

Reduces security analysis task to analyzing primitive

Confidence in stream cipher's security gives confidence in scheme's security

Candidate stream ciphers?

Build a stream cipher from scratch. Example: RC4 designed by Ron Rivest in the 1990s. Up until recently, a popular custom construction of stream cipher used Internet-wide
Confidence? Cryptanalysis (frequency anaysis) shows it is ***not*** pseudorandom



Block ciphers

Family of permutations, one permutation for each key

$$E : \{0,1\}^k \times \{0,1\}^n \dashrightarrow \{0,1\}^n$$

Use notation $E(K,X) = E_K(X) = Y$
Define inverse $D(K,Y) = D_K(Y) = X$ such that $D_K(E_K(X)) = X$
E,D must be efficiently computable

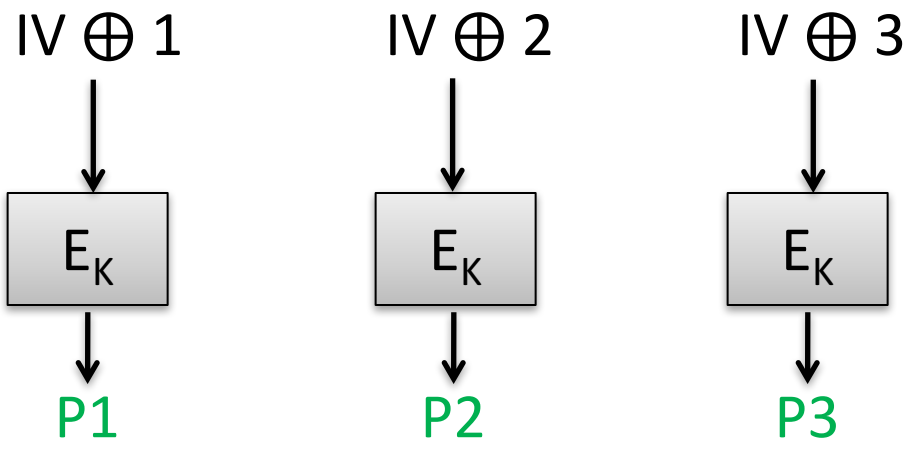
Key generation: pick K uniformly at random from $\{0,1\}^k$

Nowadays $k \geq 128$

CTR mode stream cipher

Counter mode stream cipher CT = (Kg,G) where:

- Kg outputs random k-bit key
- $G(K,IV,L) = \text{trunc}_L(\ E_K(IV \oplus 1) \| E_K(IV \oplus 1) \| \ \ldots \ \| E_K(IV \oplus m)\ )$
  where $m = \text{ceil}(|M| / n)$ and trunc_L outputs first L bits of input



Truncate P3 to get L total bits

SE from a stream cipher

Say we have a secure stream cipher. How do we build an SE scheme?

Kg():
$K \xleftarrow{\$} \{0,1\}^k$

Pick a random key

Enc(K,M):
$L \leftarrow |M|$
$IV \xleftarrow{\$} \{0,1\}^n$
Return $(IV, G(K,IV,L) \oplus M)$

Dec(K,(IV,C)):
$L \leftarrow |C|$
Return $G(K,IV,L) \oplus C$

Assume ciphertext can be parsed into IV and remaining ciphertext bits

CTR-mode SE scheme

Say we have a secure stream cipher. How do we build an SE scheme?

Kg():
$K \xleftarrow{\$} \{0,1\}^k$

Pick a random key

Enc(K,M):
$L \leftarrow |M|$; $m \leq \text{ceil}(L/n)$
$IV \xleftarrow{\$} \{0,1\}^n$
$P \leftarrow \text{trunc}_L(E_K(IV \oplus 1) \| \cdots \| E_K(IV \oplus m))$
Return $(IV, P \oplus M)$

$\text{trunc}_L( )$ outputs first L bits of input

Dec(K,(IV,C)):
$L \leftarrow |C|$; $m \leq \text{ceil}(L/n)$
$P \leftarrow E_K(IV \oplus 1) \| \cdots \| \text{trunc}(E_K(IV \oplus m))$
Return $(IV, P \oplus C)$

Assume ciphertext can be parsed into IV and remaining ciphertext bits

Block cipher security

Func(n) is set of all functions
$\{0,1\}^n \rightarrow \{0,1\}^n$

O is called an ***oracle***. A subroutine that adversary can make calls to.

PRF(E, $\mathcal{C}$):
K <-$ $\{0,1\}^k$
F <-$ Func(n)
b <-$ {0,1}
b' <-$ $\mathcal{C}^O()$
Return (b = b')

O(X):
If b = 1 then
  Return $E_K(X)$
Return F(X)

(t,q,ϵ)-pseudorandom function:
no attacker limited to time t and q queries to O can distinguish between E_K and random function with advantage greater than ϵ

Advantage:

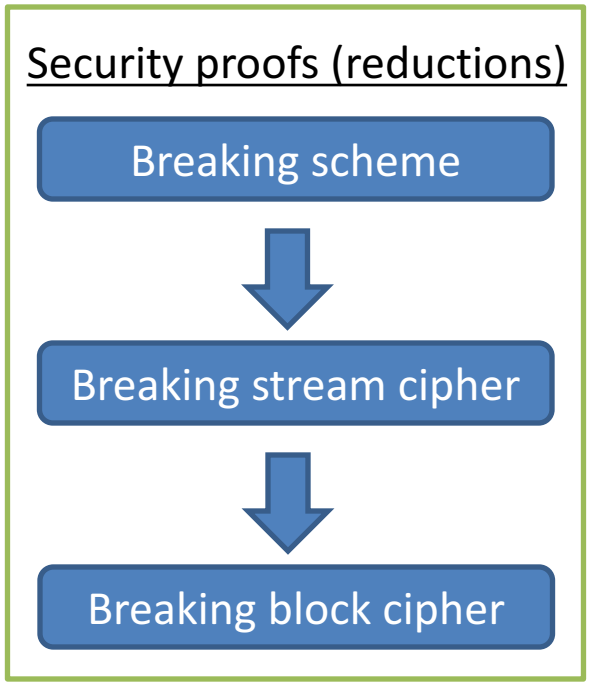
ϵ = | Pr[PRF1(G,L, $\mathcal{C}$) = 1] - Pr[PRF0(G,L, $\mathcal{C}$) = 0] |

PRF game with b fixed to 1

PRF game with b fixed to 0

Reduction-based security analysis

Goal: show that if stream cipher is secure, then encryption is secure



Attacker $\mathcal{A}$ violates
(t, ϵ)-indistinguishability security

For any $\mathcal{A}$ need to give $\mathcal{B}$ for which $t' \approx t$ and $\epsilon' \approx \epsilon$

Attacker $\mathcal{B}$ that violates
(t', ϵ')-pseudorandom generator security of G

For any $\mathcal{B}$ need to give C with $t'' \approx t'$, $\epsilon'' \approx \epsilon'$, q smallish

Attacker C that violates
(t'', q, ϵ'')-pseudorandom function security of E

Reduces security analysis task to analyzing block cipher

Confidence in block cipher security gives
confidence in scheme's security

Reduction 1

IND(SE,$\mathcal{A}$):
(st,M_0,M_1) <-$ $\mathcal{A}_1$
K <-$ Kg ; b <-$ {0,1}
C <-$ Enc(K,M_b)
b' <-$ $\mathcal{A}_2$ (st, C)
Return (b = b')

PRG(G,L,$\mathcal{B}$):
K <-$ Kg ; IV <-$ $\{0,1\}^n$
P_1 <- G(K,IV,L)
P_0 <- $\{0,1\}^L$
b <-$ {0,1}
b' <-$ $\mathcal{B}$ (IV,P_b)
Return (b = b')

$\Pr[\text{IND}(\text{SE},\mathcal{A}) = 1] = 1/2 + \epsilon$

$\epsilon' = |\ \Pr[\text{PRG1}(G,L,\mathcal{B}) = 1] - \Pr[\text{PRG0}(G,L,\mathcal{B}) = 0]\ |$

$\mathcal{B}$(IV,P):
(M_0,M_1) <-$ $\mathcal{A}$
d <-$ {0,1}
d' <-$ $\mathcal{A}$ (IV, $M_d \oplus P$)
If (d = d') then
    Return 1
Return 0

$\Pr[\text{PRG1}(G,L,\mathcal{B}) = 1] = \Pr[\text{IND}(\text{SE},\mathcal{A}) = 1]$
$\Pr[\text{PRG0}(G,L,\mathcal{B}) = 0] = \Pr[d = d' \wedge b = 0] = 1/2$

$\epsilon' = \Pr[\text{IND}(\text{SE},\mathcal{A}) = 1] - 1/2$
$= \epsilon + 1/2 - 1/2$
$= \epsilon$

$\mathcal{B}$ runs in time that of $\mathcal{A}$ plus small overhead

Reduction 2

PRG(G,L,$\mathcal{B}$):
K <-$ Kg ; IV <-$ $\{0,1\}^n$
P_1 <- G(K,IV,L)
P_0 <- $\{0,1\}^L$
b <-$ {0,1}
b' <-$ $\mathcal{B}$ (IV,P_b)
Return (b = b')

ϵ' = | Pr[PRG1(G,L,$\mathcal{B}$) = 1] - Pr[PRG0(G,L,$\mathcal{B}$) = 0] |

PRF(E,$\mathcal{C}$):
K <-$ $\{0,1\}^k$
F <-$ Func(n)
b <-$ {0,1}
b' <-$ $\mathcal{C}^O$()
Return (b = b')

O(X):
If b = 1 then
  Return E_K(X)
Return F(X)

ϵ'' = | Pr[PRF1(G,L,$\mathcal{C}$) = 1] - Pr[PRF0(G,L,$\mathcal{C}$) = 0] |

$\mathcal{C}^O$:
IV <-$ $\{0,1\}^n$
P = trunc_L(O(IV $\oplus$ 1) $\|$ $\cdots$ $\|$ O(IV $\oplus$ m))
d' <-$ $\mathcal{B}$(IV, P)
Return d'

Pr[PRF1(G,L,$\mathcal{C}$) = 1] = Pr[PRG1(SE,$\mathcal{B}$) = 1]
Pr[PRF0(G,L,$\mathcal{C}$) = 0] = Pr[PRG0(SE,$\mathcal{B}$) = 0]

$\epsilon'' = \epsilon'$

$\mathcal{C}$ runs in time that of $\mathcal{B}$ plus small overhead
$\mathcal{C}$ makes m queries to O

Summary & game plan

- Computational indistinguishability
- Stream ciphers
  - Pseudorandom generator security
- Block ciphers
  - Pseudorandom function security
- Reductions

- Next time:
  - Block cipher design