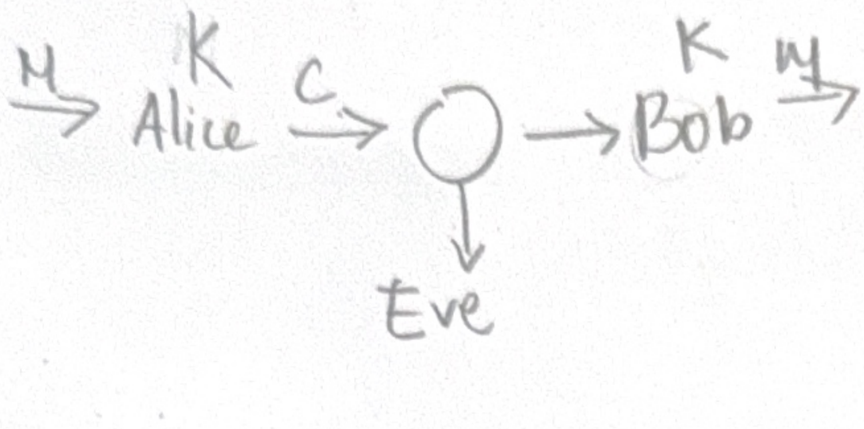
CSE 426 Intro to Encryption Lecture 2

Symmetric cryptography: sender and receiver share secret key that adversary don't know



Eve should not learn anything about M

K = secret key

M = plain text

C = cipher text

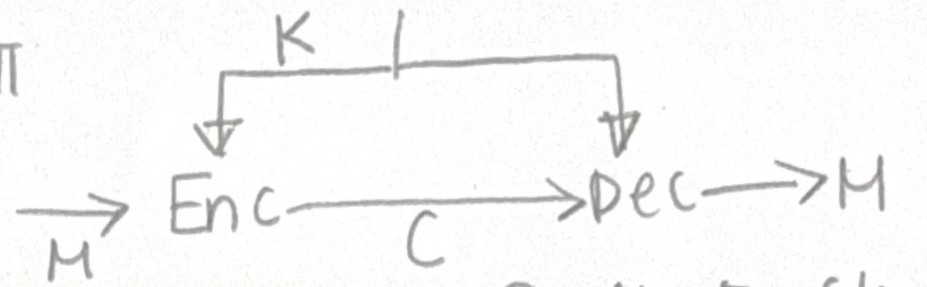
cryptographic <u>scheme</u>: a collection of algorithms to achieve a task

$a \xleftarrow{\$} \{0,1\}^n$ pick a uniformly (\$) at random from $\{0,1\}^n$

$\Pi = (Kg, Enc, Dec)$

Kg: key generation (randomized)

symmetric encryption scheme Π



$\mathcal{M}$ (plaintext space)

$= \{0,1\}^*$ or $\{0,1\}^n$

$Dec(K, Enc(k, M)) = M$

* <u>A randomized algorithm can use randomness but does not need to</u>

<u>correctness</u> & <u>security</u> are defined separately

$Dec(K, Enc(K,M)) = M$ $\quad \mathbb{P}(M=m \mid C=c)$ should be same for all $m \in M$

~~Example: mono-alphabetic substitution~~

Total of 26! keys

not secure: English language, especially for 2,3 lettered words

frequency of alphabets

Kerckhoff's Principle: everything except the key is public knowledge

Ciphertext-only attack: only see ciphertext and try to retrieve info about plaintext

<u>Attack</u> is successful as long as we recover some info

Secure encryption scheme: hide all possible information

$K \xleftarrow{\$} Kg$

CSE 426 Cryptography Perfect Secrecy Lecture 3

One-time pad $C \leftarrow M \oplus K$

ciphertext-only attack

Shannon Secrecy: $\Pr_{K \xleftarrow{\$} Kg, M \xleftarrow{\$} D}[M = M^* \mid Enc(K, M) = C^*] = \Pr_{M \xleftarrow{\$} D}[M = M^*]$

for all $M^* \in \mathcal{M}$ and $C^* \in \mathcal{C}$

Notation

$V \xleftarrow{\$} D$ sample V from D

Perfect secrecy: $\Pr_{K \xleftarrow{\$} Kg}[Enc(K, M_0) = C] = \Pr_{K \xleftarrow{\$} Kg}[Enc(K, M_1) = C]$

for all pair $M_0, M_1 \in \mathcal{M}$ and ciphertext $C \in \mathcal{C}$

perfect secrecy ≡ Shannon secrecy

Theorem: One-time pad satisfies perfect secrecy

proof: for all $M, C \in \{0,1\}^n$

$$\Pr_{K \xleftarrow{\$} Kg}(Enc(K, M) = C) = \Pr_{K \xleftarrow{\$} \{0,1\}^n}[M \oplus K = C] = \frac{1}{2^n}$$

Q.E.D.

Theorem: Perfect secrecy requires $|K| \geq |M|$

proof: AFTSOC $|K| < |M|$

Pick $M^* \in \mathcal{M}$

$Enc(M^*) := \{C \mid \exists K \in K : Enc(K, M^*) = C\}$

$|Enc(M^*)| \leq |K|$

pick C^* from $Enc(M^*)$

$Dec(C^*) := \{M \mid \exists K \in K : Dec(K, M^*) = M\}$

$|Dec(C^*)| \leq |K| < |M|$, pick $M^{**} \in M \setminus Dec(C^*)$

then $\Pr_{K \xleftarrow{\$} Kg}(Enc(K, M^{**}) = C^*) = 0$

> consequence: perfect secrecy not practical

CSE 426 Lecture 8: Proving IND-CPA security

ind-cpa advantage $Adv_{\pi}^{ind\text{-}cpa} = |Pr[D^{LR_0[\pi]} \Rightarrow 1] - Pr[D^{LR_1[\pi]} \Rightarrow 1]|$

1$CTR

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

$Enc(K, M)$
$R \xleftarrow{\$} \{0,1\}^n$
$C \leftarrow (R, E(K,R) \oplus M)$
return C

$Dec(K, C)$
$(R, C') \leftarrow C$
return $C' \oplus E(K,R)$

Prf advantage of D against E

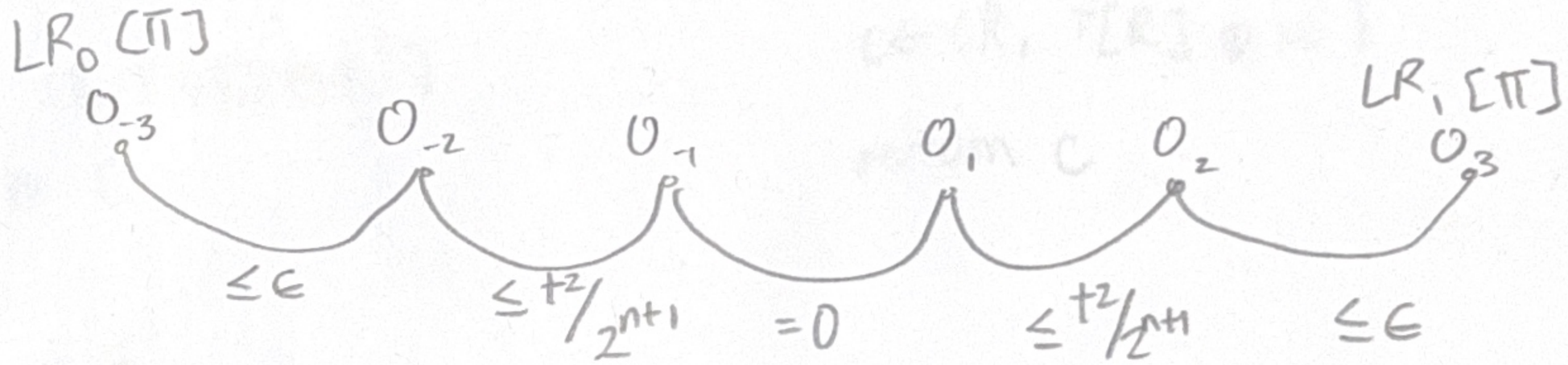
$$Adv_E^{prf} |Pr[D^{KF[E]} \Rightarrow 1] - Pr[D^{RF[n]} \Rightarrow 1]|$$

block cipher $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

Theorem: If E is a (t, ϵ) PRF then 1$CTR (t, δ) IND-CPA secure where $\delta = 2\epsilon + t^2/2^n$.

Corollary 1: If $n = \omega(\log k)$ and $E = PRF$ then 1$CTR is IND-CPA secure

Corollary 2: If $n = \omega(\log k)$ and $E = PRP$ then 1$CTR is IND-CPA secure



$$Adv_{\pi}(D) = Adv^{dist}_{O_{-3}, O_3}(D)$$

$$\leq \sum_{i=-3}^{2} Adv^{dist}_{O_i O_{i+1}}(D)$$

O_3:
$\lfloor R_0, [\Pi]$
$R \xleftarrow{\$} \{0,1\}^n$
$C \leftarrow (R, E(K,R) \oplus M^0)$
return C

O_3:
$\lfloor R_1, [\Pi]$
...
$C \leftarrow (R, E(K,R) \oplus M^1)$
return C

O_2:
...
$C \leftarrow (R, T[R] \oplus M^1)$
return C

O_{-2}:
$R \xleftarrow{\$} \{0,1\}^n$
If $T[R] = \perp$ then $T[R] \xleftarrow{\$} \{0,1\}^n$
$C \leftarrow (R, T[R] \oplus M^0)$
return C

$O_{-3} \rightarrow O_{-2}$: not easier than distinguishing E from RF
then $Adv^{dist}_{O_{-3}, O_{-2}}(D) \leq \epsilon$

O_{-1}:
$R \xleftarrow{\$} \{0,1\}^n$
$T[R] \xleftarrow{\$} \{0,1\}^n$
$C \leftarrow (R, T[R] \oplus M^0)$
return C

O_1:
...
$C \leftarrow (R, T[R] \oplus M^1)$
return C

$O_3 \rightarrow O_{-2} \leq \epsilon$
O^F that calls either O^{-3} or O^{-2} $O^{KF[E]} \equiv O_{-3}$, $O^{RF[n,n]} \equiv O_{-2}$

$Pr[D^{O^{-3}} \Rightarrow 1] = Pr[D^{O^{KF[E]}} \Rightarrow 1] = Pr[(D^\circ)^{KF[E]} \Rightarrow 1]$

$Pr[D^{O^{-2}} \Rightarrow 1] = Pr[D^{O^{RF[n,n]}} \Rightarrow 1] = Pr[(O^\circ)^{RF[n,n]} \Rightarrow 1]$

then $Adv^{dist}_{\Sigma^3, \Sigma^2}(D) = Adv^{dist}_{\Sigma^{F[E]}, \Sigma^{F[n,n]}}(D^\circ) = Adv^{prf}_{E}(D^\circ)$

which is (t, ϵ)

Fact 3: $Adv^{dist}_{\Sigma^2, \Sigma^1}(D) \leq \frac{t^2}{2^{n+1}}$

$Adv^{dist}_{\Sigma^2, \Sigma^1}(D) \leq P^{IV}_{coll}(t, \{0,1\}^n) \leq \frac{t^2}{2^{n+1}}$

CSE 426 Lecture 9: Modes of Operation + Active Attacks

$KF \to \{0,1\}^K$ $RF[M,N] \to$ permutation

prf advantage

$$Adv_{\pi}^{prf}(D) = |Pr[D^{KF(\cdot)} \Rightarrow 1] - Pr[D^{RF[m,n]} \Rightarrow 1]|$$

$Adv^{dist}_{O_1,O_1}(D) = 0$ since XOR is perfectly secure

then $\delta = 2\varepsilon + t^2/2^n$

Need to relax def of IND-CPA security to adapt to arbitary length message

ex: if $|M^0| < |M^1|$ then $|C^0|$ probably $< |C^1|$ then we break IND-CPA security

$LR_b(M^0, M^1)$ if $|M_d| \neq |M_1|$ return $\perp$

fingerprinting attack: utilize message length

Counter Mode Encryption ($CTR)

Cipher block chaining ($CBC)

Increase string, treat $X \in \{0,1\}^n$ as integer

when overflow, truncate

CBC (cipher block chaining)

$M[1], \cdots, [M[l]$

$IV \xleftarrow{\$} IV \in \{0,1\}^n$

- can utilize parallelization

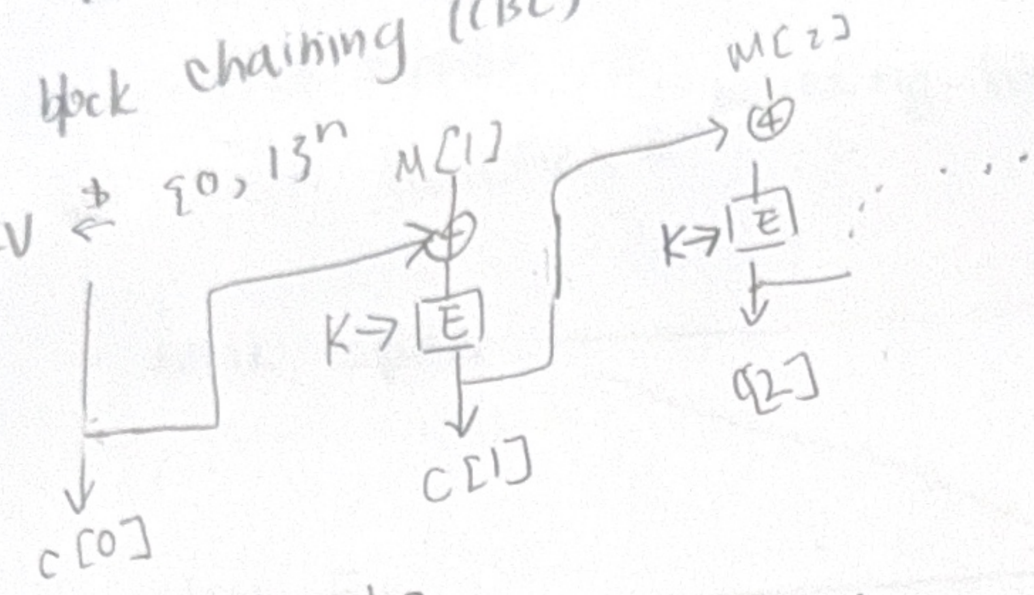
for $i = 1$ to l

$p[i] \leftarrow E(K, IV+i)$

$C[i] \leftarrow M[i] \oplus p[i]$

return $C[0]C[1] \ldots C[l]$

cipher block chaining (CBC)



for i=1 to ℓ do

$C[i] \leftarrow E(K, M[i] \oplus C[i-1])$

return $C = C[0]\, C[1] \cdots C[\ell]$

Goal: efficiently computable and efficient padding $\{0,1\}^* \to (\{0,1\}^n)^+$

Adding 0 → what if M ends with 0, not invertible

PKCS #7 padding

how many $k \in \{1, \ldots, n-1\}$ are missing

pad k copies of k

problematic padding

CSE 426 midterm review

- block cipher
- hash function

← building blocks

block cipher → symmetric encryption schemes

Hash Func. → Message Authentication Codes

Block cipher: $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ s.t. $\forall K \in \{0,1\}^k$

$E_K: X \to E(K, X)$ is a permutation

Message Authentication Code: $\{0,1\}^k \times \{0,1\}^* \to \{0,1\}^t$

Hash fn: $\{0,1\}^s \times \{0,1\}^* \to \{0,1\}^t$

- Symmetric Encryption

  Π (Kg, Enc, Dec)

- Define Oracle

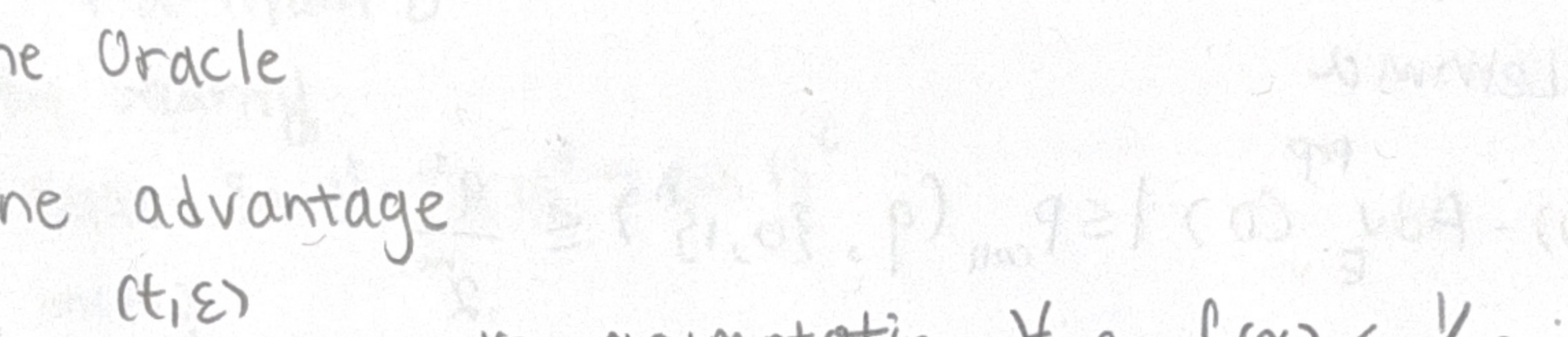
- Define advantage

  (t, ε)

- Concrete security vs asymptotic $\forall c \; f(x) \leq 1/x^c$ for $\forall x > x_0$

General Oracle Model

- Oracle O



PRP security

$$Adv_E^{prp}(D) = |Pr[D^{KF[E]} \Rightarrow 1] - Pr[D^{RP[n]} \Rightarrow 1]|$$

KF [E]
- init ()
- Eval (X)
  - return E(K, X)

RP[n]
- init ()
  - $S \leftarrow \phi$
  - T ← empty dict
- Eval
  - if T[X] = ⊥ then
    - $T[X] \xleftarrow{\$} \{0,1\}^n \setminus S$
    - $S \leftarrow S \cup T[X]$
  - return T[X]

"not very different from random permutation"

PRF security

$T[X] \xleftarrow{\$} \{0,1\}^n$

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

$D^{RF[m,n]} \Rightarrow 1$

Switching Lemma

$$|Adv_E^{prf}(D) - Adv_E^{prp}(D)| \leq P_{coll}(q, \{0,1\}^n) \leq \frac{q^2}{2^{n+1}}$$

corollary: if $n = \omega(\log k)$ then E is PRP iff E is PRF

IND-CPA security

$$Adv_\Pi^{ind\text{-}cpa}(D) = |Pr[D^{LR_0[\Pi]} \Rightarrow 1] - Pr[D^{LR_1[\Pi]} \Rightarrow 1]|$$

assume $|M_0| = |M_1|$

Collision resistance (CR)

CR[H]

init()

$S \xleftarrow{\$} \{0,1\}^s$

Fin(M_1, M_2)

if $M_1 \neq M_2$ and $H(S, M_1) = H(S, M_2)$ return 1

else return 0

$Adv^{cr}_H(A) = Pr[A^{CR[H]} \Rightarrow 1]$

2nd Preimage Resistance (2PR)

init()

queried $\leftarrow 0$; $S \xleftarrow{\$} \{0,1\}^s$

Msg(M)

if queried = 0 then

queried = 1 ; $M_1 \leftarrow M$

return S

Fin(M_2)

if queried = 1 and $M_1 \neq M_2$ and $H(S, M_1) = H(S, M_2)$ return 1

else return 0

only give seed after give message

UF-CMA Security

MAC: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^l$

init()

$Q \leftarrow \phi$

$K \xleftarrow{\$} \{0,1\}^k$

Eval(M)

$Q \leftarrow Q \cup \{M\}$

return MAC(K, M)

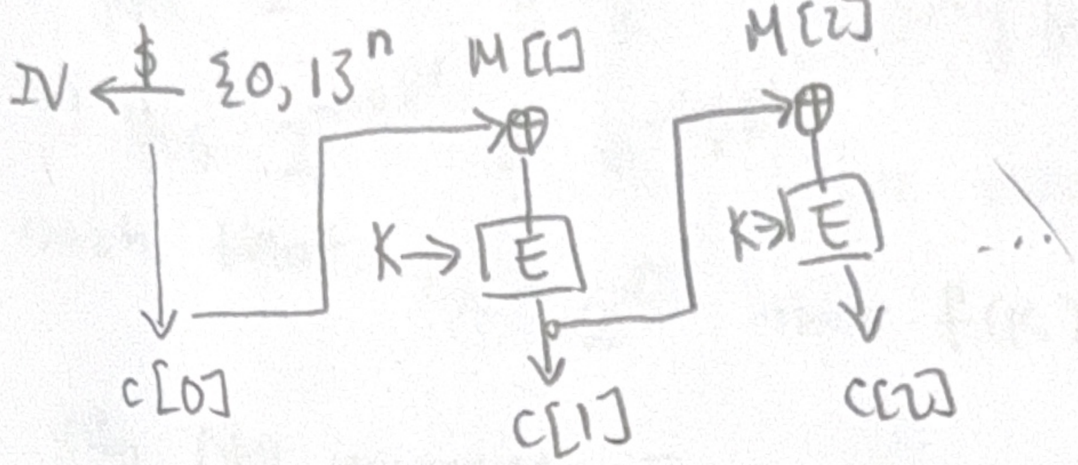
Fin(M^*, T^*):

if $M^* \notin Q$ and $MAC(K, M^*) = T^*$ return 1

else return 0

4/26 Active Security & Padding Oracle Attack

Cipher block chaining



PKCS #7 padding

- how many bytes missing to make multiple of 16 fill K copies of K

- public server allow attacker to send c' and learn potential

By changing a byte in last block ish, we can make the padding invalid

If last byte of padded plaintext is X & we make last byte of and ciphertext block to $X \oplus Y \oplus 01$ (makes last byte 01), we will always have a valid padding.

& if we make it $X' \neq X \oplus Y \oplus 01$, padding will always be invalid!

"~~impossible~~ infeasible to create new ciphertext that is valid" even after seeing valid ciphertext of same key

INT-CTXT Security

INT-CTXT + IND-CPA $\Rightarrow$ CCA security

Midterm 1 practice

Task 1

a) No, $2^{-3\log(K)} = K^{-3}$. Clearly for $c > 4$, $1/K^c < 1/K^3 = f(K)$

b) Yes $2^{-\log K^3} = K^{-\log K^2}$ for any c $\log K^2 < c$ find K_0 such that $K_0 > 2^{\sqrt{c}}$ then $f(K) > 1/K^c$

c) No. Not invertible. For instance if $K = 0^n$ then $E(K, X) = 0^n$ for all X.

d) Yes remove all 0 until you see 1

Task 2

a) Yes. If it is not PRF, then there is distinguisher we can inverse F_1 and distinguish F

b) No.

D^O

$M_1 \leftarrow 0^n \| 0^n$

$M_2 \leftarrow 0^n \| 1^n$

$C_1 \| C_2 \leftarrow O.\text{Eval}(M_1)$

$C_3 \| C_4 \leftarrow O.\text{Eval}(M_2)$

if $C_1 = C_4$ return 1

else return 0

c)

D^O

$X_1 \leftarrow 0^n$ $X_4 \in 1^n$

$X_2 \leftarrow 0^n$ $X_5 \leftarrow 1^n$

$X_3 \leftarrow 1^n$ $X_6 \leftarrow 1^n$

if $O.\text{Encrypt}(X_1 \| X_2 \| X_3)$

$= O.\text{Encrypt}(X_4 \| X_5 \| X_6)$

then return 1

else return 0

Task 3

$C[0]$ $C[1]$ -- $C[\ell] \leftarrow C$

a) for i in range $[1, \ell]$:

$M[i] \leftarrow AES^{-1}(k, C[i]) \oplus AES(K_2, C[0])$

For $LR_1[\Pi]$ to return 1, 60%.

b)

$C_0 \| C_1 \| C_2 \leftarrow O.\text{Encrypt}(0^{16} \| 1^{16}, 0^{16} \| 0^{16})$

if $C_1 = C_2$ then return 1

else return 0

Notice for $LR_0[\Pi]$ to return 1, $AES(K_1, 0^{16}) \oplus AES(K_2, R))$

$= AES(K_1, r^{16}) \oplus AES(K_2, R))$

which is negligible.

c)

After applying $AES^{-1}(K_1, C[i])$ This is equivalent roughly to 1$ CTR, which is IND-CPA secure.

Task 4.

a) Find $2^{n/2}$ samples s.t. they collide

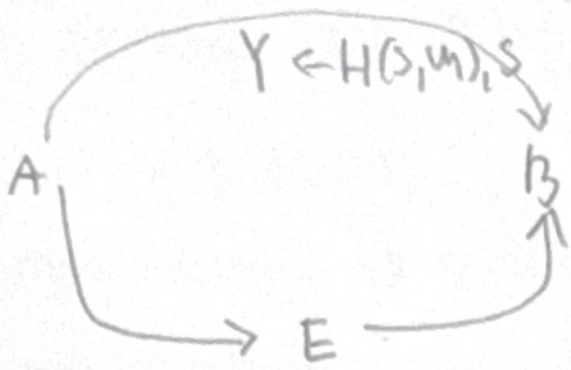
b) n is 128 so it takes 2^{64} to break which is feasible

c) ~~Part a no longer work because~~

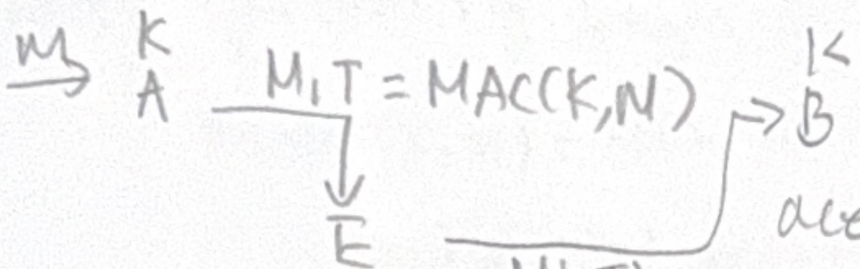
Can't pre-compute

CSE 426 Message Authentication Codes

unreliable channel



accept if $H(S, M') = Y$ to authenticate message



accept M' iff $Mac(K, M') = T'$

→ Def of MAC security (UF-CMA) unforgeability under chosen-message Attack

init():
$Q \leftarrow \phi$, $K \xleftarrow{\$} \{0,1\}^K$

Eval(M):
$Q \leftarrow Q \cup M$
return MAC(K, M)

Fin(M^*, T^*):
if $M^* \notin Q$ and $MAC(K, M^*) = T^*$ return 1
Else return 0

$MAC: \{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^l$

If F is $\alpha(t, \varepsilon)$ PRF then it is also (t', δ)-UF-CMA secure for $\delta = \varepsilon t \frac{1}{2^l}$ and $t' \approx t$. $(l = \omega(\log k))$

Pf: Give O s.t.

$O^{RF[F]} \equiv UF\text{-}CMA[F]$

$Pr[A^{O^{RF[*,l]}} \Rightarrow 1] \leq \frac{1}{2^l}$ for all A → $O^{kF[F]}$

$Pr[A^{O^{RF[F]}}]$
$\leq |Pr[A^{O^{kF[F]}} \Rightarrow 1] - Pr[A^{O^{RF[*,l]}} \Rightarrow 1]| + Pr[A^{O^{RF[*,l]}} \Rightarrow 1]$
$\leq |Pr[A^{O^{kF[F]}} \Rightarrow 1] - Pr[A^{O^{RF[*,l]}} \Rightarrow 1]| + \frac{1}{2^l} = Adv^{PR}(A^O) + \frac{1}{2^l}$

Hash then encrypt

$$F((K,s),x) = E(K, H(s,x))$$

CSE 426 Lecture 14 Authenticated Encryption

MAC(K, M) = H(S, K||M)

strongly related to length extension attack

Given T=H(S, X) compute H(S, X||Y) from T, S, Y without knowing X

HMAC (preventing length-extension attack)

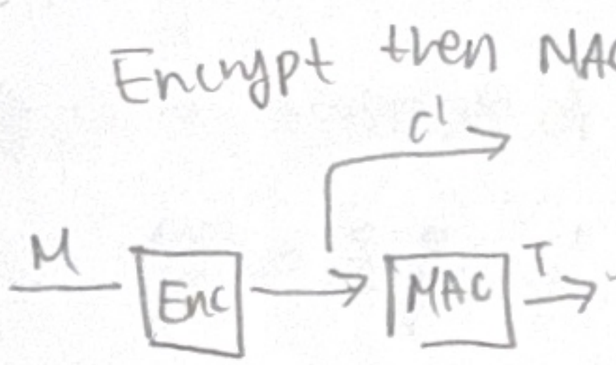
HMAC (K, M) = H(S, K ⊕ opad || H(S, K ⊕ ipad || M))

ipad ≠ opad and are constants

ciphertext security

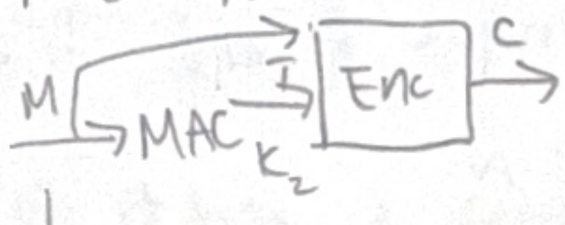
Authenticated Encryption: IND-CPA & INT-CTXT ⇒ CCA security (chosen-ciphertext Attack)

Encrypt then MAC



ciphertext security

MtE



plaintext integrity (INT-PTXT)

- keep track of plaintext
- can send info that Alice already sent! with different ciphertext

need to forge MAC with Dec

↓

checking string equality reveals which byte is problematic

↓

can fail Dec & MAC so by measuring time adversary can know where

CSE 426 Lecture 16 Number Theory

Alice and Bob agree on key while Eve sees everything

$\{X, Y, K\} \approx \{X, Y, K'\}$

Group

$(G, *)$ set of elements G with binary operation

1. closure
2. identity
3. associativity
4. inverse $(\forall a \in G, \exists b \in G)\ a * b = b * a = 1$

multiplication is not a group

"Hard" = $O(|G|)$ "easy" = $O(\log |G|)$

Theorem

any $a \in N$ with $N > 0$ $\exists$ unique q and r s.t.

$a = Nq + r$ and $0 \leq r < N$

Z_{15}^* → number coprime to 15

$|Z_{15}^*| = \phi(15)$

any prime $\phi(p) = p - 1$

p, q $\phi(pq) = (p-1)(q-1)$

$\phi(N) = \prod p_i^{k_i - 1}(p_i - 1)$

CSE lecture 17

BinPow (Square and Mult.)

$e = e_k e_{k-1} \cdots e_0$

$z \leftarrow 1$

for $i = k$ down to 0 do

$z \leftarrow z^2$

if $e_i = 1$ then

$z \leftarrow z * x$

return z

$\forall x \in \mathbb{Z}_N^*, \; x^{\phi(N)} = 1$

$x^e \equiv x^{e \bmod \phi(n)} \pmod N$

Corollary of Lagrange's: $\forall x \in G, \; x^{|G|} = 1$

for any group $(G, *)$

$\langle x \rangle = \{x^e \mid e \in \mathbb{N}\} = \{x^e \mid e \in \mathbb{Z}_{|G|}\} \subseteq G$

$(\langle x \rangle ; *)$ is also a group

g is a generator of G if

$\langle g \rangle = \{g^0 = g^1, \cdots, g^{|G|-1}\} = G$

A Group G is cyclic iff it has a generator

Z_n^* is cyclic iff $N = 2, 4, p^k, 2p^k$ where p is an odd prime

Discrete Logarithm

$G = \langle g \rangle$, let $N = |G|$

Ex 4.6 lecture 18 Diffle-Hellman Key Exchange

$|\langle X \rangle|$ generated is often $|N|$ factor of

$x \xleftarrow{\$} \mathbb{Z}_m$, $X = g^x$ $\xrightarrow{X}$ $\xleftarrow{Y}$ $y \xleftarrow{\$} \mathbb{Z}_m$, $Y = g^y$

$K = Y^x = g^{xy} = X^y$

Ever see big X and big Y

breaking key exchange for discrete log

if discrete log is easy then Diffle-Hellman Key Exchange is easy

DL [G, g]:

Fin(x):
If $X = g^x$ then return 1
else return 0

Init()
$X \xleftarrow{\$} G$
return X

$Adv^{DL}_{G,g}(A) = Pr[A^{DL[G,g]} \Rightarrow 1]$

CDH → DL yes

DL → CDH ?

CPH [G, g]:

$x, y \xleftarrow{\$} \mathbb{Z}_{|G|}$
return $X = g^x$, $Y = g^y$

$Adv^{CDH}_{G,g}(A) = Pr[A^{CDH[G,g]} \Rightarrow 1]$

Fin(Z)
return $Z = g^{xy}$

↳ not enough because adversary might learn more ex: bit digit

Decisional Diffie-Hellman

INH()
$x, y \xleftarrow{\$} R_{IG1}$
$X \leftarrow g^x$
$Y \leftarrow g^y$
$Z \leftarrow g^{xy}$
return (X, Y, Z)

INR
$x, y, z \xleftarrow{\$} R_{IG1}$
$Z \leftarrow g^z$
return (X, Y, Z)

$$Adv^{ddh}_{G,g}(D) = |Pr[D^{DDH \circ [G,g]} \Rightarrow 1] - Pr[D^{DDH, [G,g]} \Rightarrow 1]|$$

DL ← CDH ← DDH

How to choose G_q for DHKE

Z_N^* is cyclic iff $N = 2, 4, p^k, 2p^k$

$\phi(N) = 1, 2, p^{k-1}(p-1), p^{k-1}(p-1) \Rightarrow$ all even

1: DDH is easy in any G_q with even order