## SYMMETRIC SETTING

: The encryption/decryption procedure would both depend on the same shared key.

**PRIVACY**: Make sure that when an adversary obtains a ciphertext, they know nothing about the plaintext.

## ASYMMETRIC/PUBLIC KEY SETTING

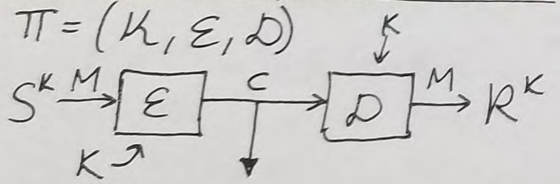
: A party possesses a pair of keys (public key + secret key). PK is known and is bound to its entity.

**MSG AUTHENTICITY**: Identify who sent the message.

| | MSG PRIVACY | MSG AUTHEN |
|---|---|---|
| Sym sett | symmetric encryption | MAC msg auth code |
| Asym/ PK sett | asymetric-pk encryption | Digital Signature |

## SYMMETRIC ENCRYPTION SCHEME

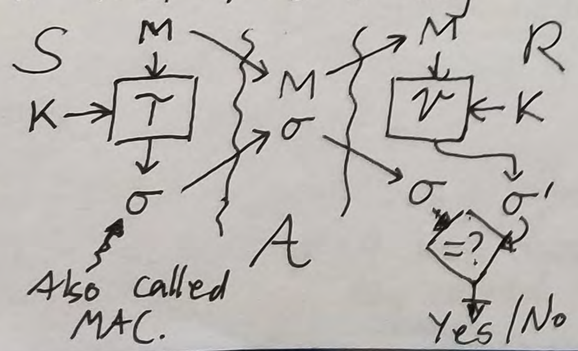
$\Pi = (K, \mathcal{E}, \mathcal{D})$




→ $2^{-n}$ probability if A were to guess string (binary) given length n.

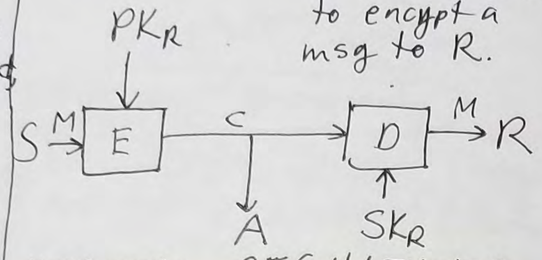
## MESSAGE AUTHENTICATION CODE

$\Pi = (K, T, V)$ $\sigma$ = tag



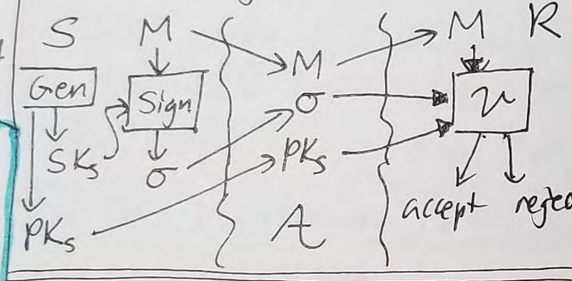

## ASYMMETRIC ENCRYPT SCHEME

$\Pi = (K, \mathcal{E}, \mathcal{D})$. S is able to find $PK_R$ and use it to encrypt a msg to R.



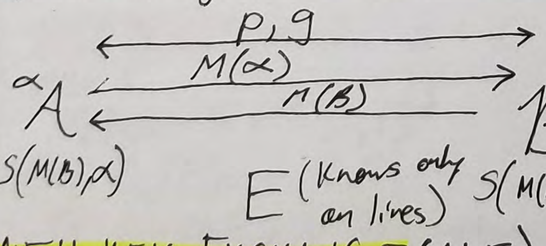

## DIGITAL SIGNATURES

$\Pi = (K, Sign, V)$



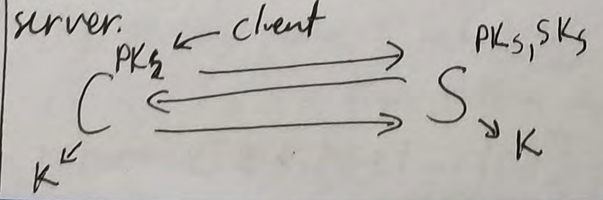

## SECRET KEY EXCHANGE (SKE)

1) S + R agree to a common value ($p=23$, $g=5$)
2) S + R generate their own secret values. {$\alpha$, $\beta$}
3) They exchange in public,
4) Process their received keys w/ their own keys.
5) Should get shared secret




## AUTH KEY EXCHANGE (AKE)

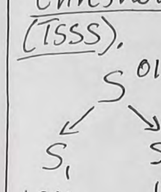
· Adversary becomes an active agent but it cannot act as a client or server.




## SECRET SHARING

***1-out-of-2 method***

$k=1$, $n=2$: Create n shares and you only need 1 to get the message. AKA: k-out-of-n threshold secret sharing scheme (TSSS).




Given $S_1$ or $S_2$ only ppl only know it's a randomly chosen bit.

* share(S) // $s \in \{0,1\}$
$S_1 \leftarrow \{0,1\}^4$
$S_2 \leftarrow S \oplus S_1$
return $(S_1, S_2)$

* recover($S_1, S_2$)
if $S_1 =$ [redacted] or $S_2 =$ [redacted]:
return 1
return $S_1 \oplus S_2$ = S

***Shamir Secret Sharing***

Based on the idea that k points are needed to define a k-1 degree of a polynomial.

Ex Prepare 3 k out of n 3. k=3, n=6

$f(x) = S + a_1 x + a_2 x^2 \dots = S_{(x)}$
↑ aka $a_0$

→ Construct 6 points using $f(0), f(1), f(2), \dots f(5) = \langle n, f(n) \rangle$
→ Reconstruct 3 points is enough)

$(x_0, y_0)$; $(x_1, y_1)$; $(x_2, y_2)$

$$l_0 = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = ax^2 - bx + c$$

$$l_1 = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = dx^2 - ex - f$$

$$l_2 = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = gx^2 - hx - i$$

Then

$$f'(x) = \sum_{j=0}^{2} y_j \cdot l_j(x)$$

$$= y_0 l_0 + y_1 l_1 + y_2 l_2$$

Simplify!

$S = f'(0)$

## FINITE FIELD / GALOIS F

→ iff exists if have $p^m$ elements
p = prime m = + integer

Ex 11 elements: GF(11)
81 elements: $GF(81) = GF(3^4)$
256 elements: $GF(256) = GF(2^8)$

· $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
· Must satisfy $a \cdot a^{-1} = 1 \bmod p$ given $a \in GF(p)$
* w/ polynomials

$0 \Rightarrow 0$
$1 \Rightarrow 1$
$10 \Rightarrow x$
$11 \Rightarrow x+1$
$100 \Rightarrow x^2$
$101 \Rightarrow x^2+1$
and so on...

The irreducible polynomial is the function (or bit config in the form of a function) that we divide our final answer of, lets say, $(x^2+1)(x^2)$.

## COMMITMENT SCHEME

· Alice puts her bits in an envelop and sends to B
· B announces his bits
· A helps B open envelop send.

Results based on bits $A \oplus B$

Ex mod a fraction

$k = \frac{a}{b} \pmod n$ so, $bk = a \pmod n$

Find k.

## PERFECT PRIVACY

$\forall M_0, M_1 \in \mathcal{M} \quad \forall C \in \mathcal{C}$

$Pr_K[\mathcal{E}_K(M_0) = C] = Pr_K[\mathcal{E}_K(M_1) = C]$

· An encryption scheme is perfect if the two messages are indistinguishable when encrypted
· Ciphertext contains no information about the plaintext. Access is bad. Move

w/ Adversay: $Pr[PrivK^{eav}_{A,\Pi} = 1] = \frac{1}{2}$
Can it do better than 0.5?

## OTP(K) = (K, E, D)

↳ sym. enc. scheme.

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

Alg E(K, M) // $M = \{0,1\}^k$
return $K[1 \dots |M|] \oplus M$

Alg D(K, C)
return $K[1 \dots |C|] \oplus C$ // if $\mathcal{E} = \{0,1\}^k$

NOTES:
→ |K| should NOT be shorter than |M|.

### DEF (Syntax) Sym Enc Scheme

$\Pi = (K, E, D)$ where...
* K: no input, outputs string
* E (deterministic)(stateless): takes $K \in \mathcal{K}$, $M \in \mathcal{M}$, and outputs $C \in \mathcal{C}$
* D (det, stateless): takes $K \in \mathcal{K}$ $C \in \mathcal{C}$, and outputs $M \in \mathcal{M} \cup \{\perp\}$

### SHANNON PRIVACY THEOREM

Given that $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$, the schem is secure iff:
1) $\forall K \in \mathcal{K}$, Prob(Gen() ⇒ k) = same as all
2) $\forall m \in \mathcal{M}$ and $c \in \mathcal{C}$, $\exists$ a single $k \in \mathcal{K}$ such that $Enc_k(m) \Rightarrow C$

~~Another way:~~
$\forall M \in \mathcal{M}, \forall C \in \mathcal{C}$ s.t. $Prob[E_k(M=C)] > 0$
$(\forall M_0 \in \mathcal{M})$
$Pr[M = M_0 \mid E_k(M) = C] = Pr[M = M_0]$

### INDISTINGUISHABILITY (IND)

$\Pi = (K, E, D)$ is IND secure if

$$Pr[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot)} \Rightarrow 1] = Pr[K \xleftarrow{\$} \mathcal{K} : A^{E_K(0^{|\cdot|})} \Rightarrow 1] \quad (*)$$

$E_K(\cdot)$ ↷ A ↷ $E_K(0^{|\cdot|})$

• A must choose the correct oracle

The adversary A has an advantage probability of:

$$Adv(A) = Pr[A^{E_K(\cdot)} \Rightarrow 1] - Pr[A^{E_K(0^{|\cdot|})} \Rightarrow 1] = 0$$

(*for single query only)

For single-query: They are all equivalent {Perfect Privacy, Shannon Sec, IND} when:
→ PP: where $|M_0| = |M_1|$
→ SP: where $P(M) > 0$ and $P(M') > 0$ implies $|M| = |M'|$
→ IND: $Pr[A^{E_K(\cdot)} \Rightarrow 1] = Pr[A^{E_K(0^{|\cdot|})} \Rightarrow 1]$

(*) OTP(K) satisfies PP & IND

For all M and C:
$Pr[E_K(M) = C] = 2^{-|M|}$ if $|C| = |M|$

### → Multiquery IND

• Deterministic, stateless encryption cannot achieve this {i.e. OTP(K)}
• For OTP(K) to have reasonable, good enc scheme, we must make it stateful, and/or probabilistic. ∴ OTP(K) – upgrade → OTP*(K)

**OTP*(K):** // static $s \leftarrow 0$

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

Alg $E_K(M)$:
if $s + |M| > k$ then return $\perp$
$C \leftarrow M \oplus K[s+1 \dots s+|M|]$
$s \leftarrow s + |M|$
return C

Alg $D_K(M)$: parse C into (C, s)
if $|C| + s > k$ then return $\perp$
return $C \oplus K[s+1 \dots |C|]$

### DEF: A classical PRG is a function $g: \{0,1\}^n \to \{0,1\}^N$ where $n < N$.

A "practical" PRG is an Alg that takes in $K \in \mathcal{K}$ and outputs $\{0,1\}^\infty \setminus g(K)$

(*) $Adv_g^{prg}(A) = Pr[K \xleftarrow{\$} \mathcal{K} : A(g(K))] - Pr[Y \leftarrow \{0,1\}^N : A(Y) \not\Rightarrow 1]$

### RC4: A stream cipher. Simple and fast but contains multiple vulnerbilities.

- lacks randomness
- Uses a key and extends it w/ a PRG

K → g → g(K)

• If you try to break a PRG under an ∞ amount of time, you can definitely break it! BROKEN.

### Vernam Cipher: A cipher in which a plaintext is combined w/ a pseudorandom stream of data of the same length to generate a cipher text using XOR. If the keystream is truly random and used only once it is a OTP.

Given that PRG is a func:
$G: \{0,1\}^k \to \{0,1\}^\ell$ wher $\ell$ is either $\ell > k$ or $\ell = \infty$,
we CLAIM: Vernam[G] is IND-secure if the PRG we start from is PRG-secure.

• G is "good" PRG ⇒ Vernam[G] is IND-secure
• G is "bad" PRG ⇐ Vernam[G] is not IND-secure
• ∃ B breaks G in a PRG sense ⇐ ∃ A breaks Vernam[G] in the IND-sense

Given A, how will we construct B?

(*) REDUCTION!!! Converting an A strategy to a B strategy.

A → Rx → B

A breaks Vernam[G] in IND sense

B breaks G as a PRG

→ constructing B:
1) B is given a long str Y
2) $A^F$ has an oracle {F} that encrypts strings.
3) While $A^F$ asks F to encrypt(X): B emulates what Vernam[G] would do w/ Y being the output of the PRG.
4) A halts when its output bit b matches B's output bit b'.

Claim: $Adv_G^{prg}(B) = Adv_{Vernam(G)}^{ind}(A)$

$Adv_G^{prg}(B) = Pr[B(G(K)) \Rightarrow 1] - Pr[B(\$) \Rightarrow 1]$
$= Pr[A^{Enc(\cdot)} \Rightarrow 1] - Pr[A^{Enc(\$)} \Rightarrow 1]$
$= Adv_{Vernam(G)}^{ind}(A)$

## PSEUDORANDOM FUNCTION (PRF)

A function where:

$F: K \times \{0,1\}^n \to \{0,1\}^m$

Ex ChaCha20: $\text{Byte}^{32} \times \{0,1\}^{128} \to \{0,1\}^{512}$

$Adv_F^{prf}(A) = Pr[K \xleftarrow{\$} K : A^{F_K(\cdot)} \Rightarrow 1] -$
$Pr[R \leftarrow Func(n,m) : A^{R(\cdot)} \Rightarrow 1]$

$R \approx$ random function
$F_K \approx$ Actual/Real function

Ex How many functions are there from $n$ bits to $m$ bits? $2^{m \cdot 2^n}$

* $|Funct(n,m)| = 2^{m \cdot 2^n}$

$2^{m \cdot 2^n} \} 2^n$

$m$

## PSEUDORANDOM PERMUTATION (PRP)

A function where:

$F: K \times \{0,1\}^n \to \{0,1\}^n$

and $F_K(\cdot)$ is a permutation

Ex DES: $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$

⊛ PRF/PRP should run in constant time because constant time means that the runtime is independent of key/input. So no information of the key/input is leaked

$Adv_E^{prp}(A) = Pr[K \leftarrow K : A^{E_K(\cdot)} \Rightarrow 1]$
$- Pr[\pi \leftarrow Perm(n) : A^{\pi(\cdot)} \Rightarrow 1]$

⇒ Like PRF, the # of permutations from n bits to n bits is $2^n!$

⇒ PRP = BLKCIPHERS = Invertible

## DATA ENCRYPTION STAN. (DES)

$\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$
key plntxt cprtxt

→ Feistal cipher w/ 16 rounds
→ blockcipher / PRP
→ 56-bit key is kinda short
→ hardware-only
→ export control (outside country use)
→ Standardized obstruction
→ Avalanche effect: small change in plntxt → big cprtxt change
→ Completeness: each bit of cipher depends on many bits of plaintext

↳ Prevent world-wide use.

## CHACHA 20 No key setups!!!

$BYTE^{32} \times BYTE^{16} \to BYTE^{64}$
$\{0,1\}^{256} \times \{0,1\}^{128} \to \{0,1\}^{512}$

- Very fast in software
- Uses ARX (and-rotate-xor)
- Constant time (no tables)
- Security holps up well
- Open-design (no intelligence-agency involvement)

## ADVANCED ENCRYPTION STAN: AES

$\{0,1\}^{128}_{[192 \text{ or } 256}} \times \{0,1\}^{128} \to \{0,1\}^{128}$

- Fast in hardware! Should only be used in hardware
- Open design - Takes 10 rounds.
- Complicated process: $GF(2^8)$
  1) Substitute bytes
  2) Shift rows
  3) Mix Columns
  4) Add Row Keys

* Think of input as a 4x4 table of BYTES.

## BIRTHDAY PROBLEM: Find $C(q,N)$.

$C(q,N)$ = Prob of a collison in the experiment of throwing $q$ balls uniformly at random into $N$ bins.

Collison: 2 balls in 1 bin

Paradox: $C(q,N) \sim 1/2$ when $q \approx \sqrt{N}$ or $q \approx \sqrt{2 \ln 2}\sqrt{N}$

Claim: $C(q,N) \leq \frac{q(q-1)}{2N}$

$C(q,N) = Pr[C_1 \cup C_2 \cup \cdots C_q]$

$C_i$ = event where there is a collison when we toss $i$ balls.

$\leq Pr[C_1] + \cdots Pr[C_q]$
$\leq \frac{0}{N} + \frac{1}{N} + \cdots \frac{q-1}{N}$
$\leq \frac{0+1+\cdots q-1}{N} = \frac{q(q-1)}{2N}$ ▨

## PRF/PRP Switching Lemma

Given $E: K \times \{0,1\}^n \to \{0,1\}^n$, for any A asking at most $q$ queries

$|Adv_E^{prp}(A) - Adv_E^{prf}(A)| \leq \frac{q^2}{2^{n+1}}$

* PRP → No collisons
* PRF → Some collisons

$q \ll 2^{n/2}$

## FUNDAMENTAL LEMMA OF GAME PLAYING

If games G & H are identical until bad, then

$Adv_{G,H}^{dist}(A) = Pr[A^G \Rightarrow 1] - Pr[A^H \Rightarrow 1]$
$\leq Pr[G \text{ sets bad}]$

GAME RandFunc(n) or GAME RandPerm(n)
Oracle E(x)
if $x \in Dom(f)$ then return $f(x)$
$y \xleftarrow{\$} \{0,1\}^n$
if $y \in Ran(f)$ then bad ← true; $y \xleftarrow{\$} \{0,1\}^n \setminus Ran(f)$
$f(x) \leftarrow y$
return $y$

## MODES OF OPERATION: A way of encrypting arbitrary length messages using a blk cipher.

We go over 3:
1) CTR mode - Counter
2) ECB mode - Electronic Code Book
3) CBC mod - Cipher Block Chaining

## COUNTER MODE (CTR[E])

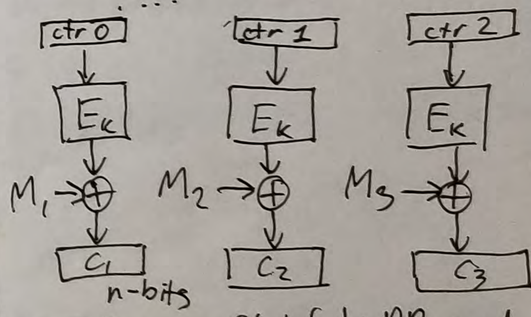
where $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

Alg K
return $K \xleftarrow{\$} K$

Alg $Enc_K(M)$
static ctr ← 0
$C \leftarrow M \oplus E_K(ctr \| 0) \| E_K(ctr \| 1) \| \cdots E_K(ctr \| (m)_n)$
(mod $2^n$ concatenate)
$C \leftarrow ctr \| C$
ctr++
return $C$

Alg $Dec(K, C)$
$ctr \| C \leftarrow C$
return $C \oplus E_K(ctr \| 0) E_K(ctr \| 1) \cdots$

$E_K$ can does not have to be PRP!




- Stateful: PP and IND-secure as long as total # of blocks queried is less than $2^n$.
- Having a CTR is CPA-secure.

* CPA-secure (Chosen Plaintext Attack): Idea that adversary can play around w/ the block cipher. $\Pi$ must be probabalistic ↳ enc scheme

$E_K + D_K$

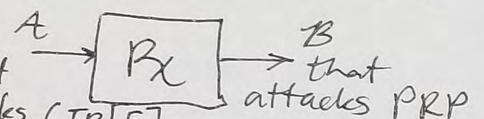
## CTR mode (continued)

↳ IND secure ← Claim:

E is a secure PRP ⇒ CTR[E] is IND secure

E is an insecure PRP ⇒ CTR[E] is not IND secure

∃B that breaks E ⇐ ∃A that breaks CTR[E]

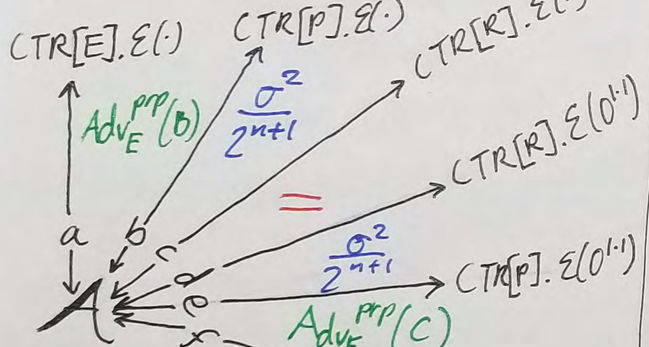



Remember: $E: K \times \{0,1\}^n \to \{0,1\}^n$

$P: Perm(n) \times \{0,1\}^n \to \{0,1\}^n$

$R: Func(n,n) \times \{0,1\}^n \to \{0,1\}^n$

→ PRPs look like PRFs once you ask a lot of questions.




advantage of adversary:

$a-f = (a-b)+(b-c)+(c-d)+(d-e)+(e-f)$

- $c=d$: A gets updated ctr or random bits. Assume no reuse
- $b-c = d-e$: Based on PRF/PRP Switching Lemma. $\sigma$ = # of queries.
- $a-b$; $e-f$: as labelled.

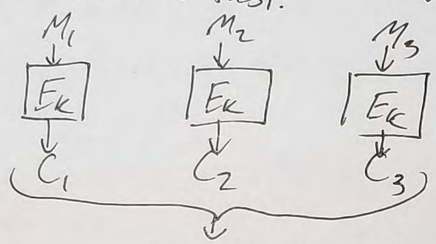
THM: E is n-bit PRP, $\pi$ = CTR[E], A is adversary to break $\pi$ that asks $\sigma$ qs. There an adversary B that gets:

$$Adv_E^{prp}(B) \geq \frac{Adv_\pi^{ind}(A)}{2} - \frac{\sigma^2}{2^{n+1}}$$

## ELECTRONIC CODE BOOK (ECB mode)

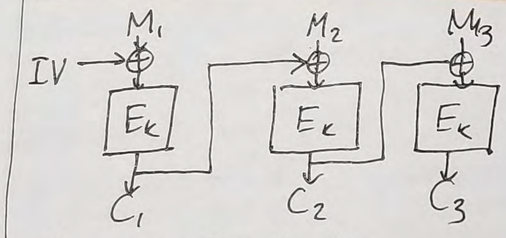
"Classical mode"

- Stateless, $E_K^{-1}$ is computable
- ↑ Deterministic! (Not CPA-secure, Not IND-secure)
- If input $M_1 = 0^n$ & $M_2 = 1^n$, you can break it fast.




Combine to get C.

## CIPHER BLOCK CHAINING (CBC)




$C \to IV || C_1 || C_2 || C_3$

IV is chosen uniformly at random so the enc. can be CPA-secure / IND-secure.

- If 0-IV, it would not be IND secure because then the scheme would be deterministic.

## KEY RECOVERY: an adversary attempt to recovery the crypographic key of an encrypt scheme

Let E be a blockcipher:

$$Adv_E^{kr}(A) = Pr[K \xleftarrow{\$} \mathcal{K}; K' \leftarrow A^{E_K(\cdot)}: K' = K]$$

- A is given $E_K(\cdot)$
- $K' = K$ is winning stmt
- Key chosen at random.

Ex If $E_K(x) = X$ then the key cannot recover. AND $Adv_E^{kr}(A) = \frac{1}{2^k}$ ← length of key

## Claim: KR secure ⇐ IND/PRP secure

KR insecure ⇒ IND/PRP secure

∃A breaks E in KR sense ⇒ ∃B breaks E in IND/PRP sense

R_K

Suppose $F = E_K$ for a random $K \xleftarrow{\$} \mathcal{K}$

Then:

$$Pr[B^{E_K} \Rightarrow 1] \geq Pr[A^{E_K} \text{ outs } K] = Adv_E^{kr}(A)$$

$$- Pr[B^{\pi} \Rightarrow 1] = \frac{1}{2^n - q}$$

$$Adv_E^{prp}(B) \geq Adv_E^{kr}(A) - \frac{1}{2^n - q}$$

## IND $ definition

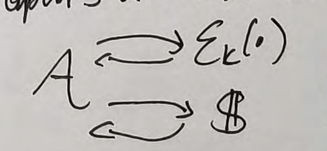
Regular IND Adv:

$$Adv_\pi^{ind}(A) = Pr[A^{E_K(\cdot)} \Rightarrow 1] - Pr[A^{E_K(0^{l \cdot l})} \Rightarrow 1]$$

New:

$$Adv_\pi^{ind\$}(A) = Pr[A^{E_K(\cdot)} \Rightarrow 1] - Pr[A^{\$^{l \cdot l + c}} \Rightarrow 1]$$

- A new oracle $\$^{l \cdot l + c}$ that just outputs a rando set of bits.




IND$ ⇒ IND

IND$ ⇏ IND

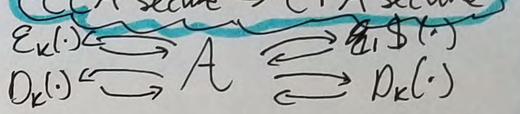
* IND$ is stronger than IND security.

- In regular IND, the fake oracle gives the encryption of $0^{l \cdot l}$ which is weaker than an encryption of $\$^{|M|+c}$

## CHOSEN CIPHERTXT ATK (CCA)

CCA secure is the notion that an enc scheme should remain secure when an adversary obtains access to the decryption func.

CCA secure ⇒ CPA secure




$$Adv_\pi^{cca}(A) = Pr[A^{E_K(\cdot), D_K(\cdot)} \Rightarrow 1] - Pr[A^{\$, D_K(\cdot)} \to 1]$$

NONMALLEABILITY: A scheme should not allow an adversary to change C to C' inducing a M' that is meaningfully related to M.

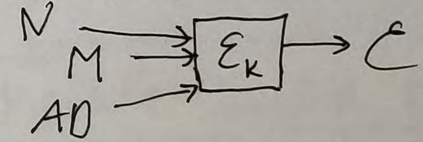
## AUTHENTICATED ENCRYPTION

A sym enc scheme should guarantee authenticity. ($\Pi = (K, \mathcal{E}, D)$)

$K \to$ probabalistic

$\mathcal{E}: \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C}$

$D: \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$




N: Nonce: arbitrary # that is used once in crypo communication

A, AD: Associative Data: Ex of packet headers. That info must be decrypted too to ensure privacy + authenticity

## DEFICIENCIES OF IND-Secure Enc

1. No random IV
2. No associated data
3. No authentication
4. Nonmalleable
5. Not include CCA

## MESSAGE AUTH. CODE (MACs)

symmetric + authentication
- Is a PRF w/ $F: K \times M \to \{0,1\}^\tau$

Let $F_K(M)$ be a $MAC_K(M)$,

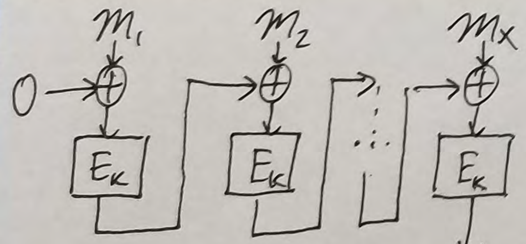
$$Adv_F^{mac}(A) = Pr[K \xleftarrow{\$} \mathcal{K}; (M,T) \leftarrow A^{F_K(\cdot)} : (M,T) \text{ is a forgery}]$$

⇒ A only knows subkeys, not key.
⇒ Forgery is (1) $T == MAC_K(M) = F_K(M)$ and (2) A never asked M

**Claim: PRF secure ⇒ MAC secure**

A MAC is similar to a PRF and since a PRF is like a random function, the prob of guessing the tag is $\frac{1}{2^\tau}$

## (raw) CBC-MAC + its insecurity




- no padding, $|M|$ is a multiple of $n$.
- VERY BAD across various lengths. Deterministic.
- fixed length messages ⇔ Secure

- A CBC-MAC using variable lengths is $\varepsilon$-AU for small $\varepsilon$.

DEF: $H: K \times \mathcal{M} \to \{0,1\}^\tau$ is **$\varepsilon$-Almost Universal** if

$$\forall M, M' \in \mathcal{M},\ M \neq M' \quad \left(\frac{1}{m}\right)$$
$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(M) = H_K(M')] \leq \varepsilon$$

## MIDTERM 1 HAPPENED

**Prop:** If $H_{K'}$ is $\varepsilon$-AU && $E_K$ is a secure PRF then $F: (\mathcal{K} \times \mathcal{K}') \times \mathcal{M} \to \{0,1\}^n$ determined by $F_{KK'}(M) = E_K(H_{K'}(M))$ is a secure PRF. (Wegman-Carter)

### Create an $\varepsilon$-AU Hash Function

- Use polynomial arith. over a $\mathbb{F}_{2^{128}}$
- Hash message $M = M_1 \dots M_m$, each block an $n$-bit key. See it as a function:

$$M(x) = x^m + M_1 x^{m-1} + \dots + M_{m-1} x + M_m$$
$$H: \mathbb{F} \times \mathcal{M} \to \mathbb{F}$$
$$H_K^\xi(M) = M(K) \qquad M - M'$$
$$Pr_K[M(K) = M'(K)] = Pr_K[g(K) = 0]$$

What's the prob that $g(K)$ will map to value 0?

$$Pr_K[g(K) = 0] \leq \frac{m}{2^n}$$

- m pts pass zero due to algebra theorem rule.

**DEF:** A nonce-based enc scheme is secure if:

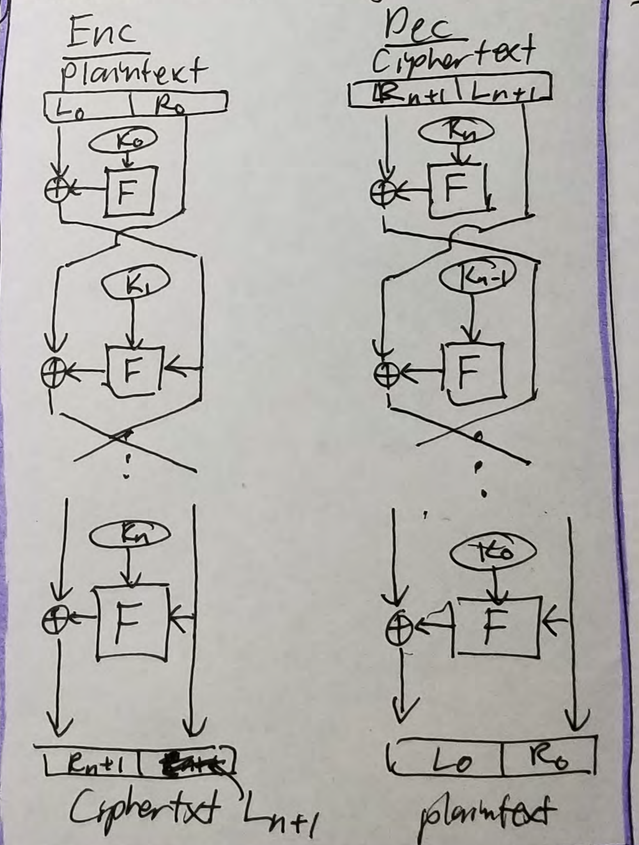
$$Adv_\Pi^{ae}(A) = Pr[A^{\mathcal{E}_K(\cdot)} \Rightarrow 1] - Pr[A^{\$(\cdot)} \Rightarrow 1]$$

and

$$Adv_\Pi^{auth}(A) = Pr[K \xleftarrow{\$} \mathcal{K}; (N,A,C) \xleftarrow{\$} A^{\mathcal{E}_K(\cdot,\cdot)} : \mathcal{D}_K(N,A,C) \neq \perp \ \&\& \ C \text{ wasn't returned from } \mathcal{E}_K(N,A,\cdot)]$$

(Forgot to add pages ago)

**FEISTEL CIPHER:** A symmetric structure used in the construction of cipher blks. Enc and Dec operations are similar, requiring only a reversal of the key schedule.




## CRYPTOGRAPHIC HASH FUNC

Takes string from a domain $H: \{0,1\}^* \to \{0,1\}^n$

$$Adv_H^{cr}(A) = Pr[(M,M') \xleftarrow{\$} A : M \neq M' \wedge H(M) = H(M')]$$

### Merkle-Damgård Construction

- Method of building collision resistant crypto. hash funcs from collision-resistant one-way compression functions.

## ASYMPTOTIC APPROACH

$G: \{0,1\}^* \to \{0,1\}^*$ where $|G(x)| > |x|$

Def: $f: \mathbb{N} \to \mathbb{R}$ is negligible if

$$(\forall c > 0)(\exists N)(\forall n \geq N)$$
$$f(n) \leq \frac{1}{n^c}$$

### Merkle-Damgård Proof

If h is collison resistan than $H = MD[w]$ is collison resistants