## G Hashing

(G.1) Defining Collision Resistance

(G.2) Birthday Attacks

(G.3) Merkle-Damgard Transform

(G.4) Designing Hash Functions from DLP

## H Key Exchange

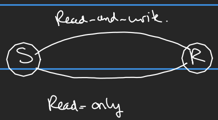
(H.1) Diffie-Helman Protocol

(H.2) DDH-assumption

---

Questions for Mids

H:




Adv. has access to both channels, and write access to one.

Challenge: You do not know which channel is read only for adv and which is read-write.

based on:
DDH Assumption
R+W access to channel by adv.

Design a protocol s.t. S, R have keys, but PPTM Adv does not, even with R+W access to any channel of their choice.

Re-wording with background

in standard scheme, there is only one channel, read only. Diffie-Hellman works.

but it fails if adversary has write access.

Once key is shared, even write access can be dealt with.

in this question, there are two channels. One is read+write for the adversary, one is read-only. we do not know which is which.

Design a protocol s.t. S, R have keys, but PPTM Adv does not, even with R+W access to any channel of their choice.

G. $h: \{0,1\}^{2n} \to \{0,1\}^{n} \xrightarrow{MDT} H: \{0,1\}^{*} \to \{0,1\}^{n}$

can be used with arbitrary compression ratios.

TODO PROOF

start with an $\underline{h}$ which is, say, $h: \{0,1\}^{3n} \to \{0,1\}^{2n}$

there should still be an MDT s.t. $H: \{0,1\}^{*} \to \{0,1\}^{2n}$

FORMALISE

F. Break the Basic-CBCMAC scheme.

↳ just take message, do CBCMAC, take answer

Replay Attacks are allowed

Q: Why?

big aside on "what is theory"

G. OWF $\Leftrightarrow$ PRG $\Leftrightarrow$ PRF $\Leftrightarrow$ MAC $\Leftrightarrow$ hashing $\Leftrightarrow$ block cipher.

Q: Start somewhere, build everything else.

---

Solutions

1. Encryption scheme : $\langle$ Gen, Enc, Dec, M $\rangle$

**Shift Cipher**

$$Gen := k \xleftarrow[R]{} [0,25]$$

$$Enc := c_i = (m_i + k) \% 26$$

$$Dec := m_i = (c_i - k) \% 26$$

$$M = [a,z]^*$$

**Substitution cipher**

$$Gen := k \leftarrow \text{Permutation of } a \dots z$$

$$Enc := c_i = k(m_i)$$

$$Dec := m_i = k^{-1}(m_i)$$

$$M = [a,z]^*$$

k: $a \to c$

$b \to n$

**Vigenere cipher** (key length $l$)

$$Gen := k \xleftarrow[R]{} [0,25]^l$$

$$Enc := c_{ln+i} = (m_{ln+i} + k_i) \% 26 \mid n \in W$$

$$Dec := m_{ln+i} = (c_{ln+i} - k_i) \% 26 \mid n \in W$$

$$M = [a,z]^*$$

2. let an alphabet permutation be $p: [a,z] \to [a,z]$

Key: $P_1 P_2 \dots P_t$

1. If we know key length

- separate cipher text into t buckets :

| | | | |
|---|---|---|---|
| $c_1$ | $c_{t+1}$ | $c_{2t+1}$ | ... |
| $c_2$ | $c_{t+2}$ | $c_{2t+2}$ | |
| ⋮ | ⋮ | ⋮ | |

- For each bucket, use frequency analysis attack
  - count all character frequencies.
  - sort characters by frequencies
  - sort alphabet by known real-world frequencies

} line up, form the key.

2. Finding key length :

3. Perfect secrecy: $P(M=m \mid C=c) = P(M=m)$

$$\frac{P(C=c \mid M=m)\, \cancel{P(M=m)}}{P(C=c)} = \cancel{P(M=m)}$$

$$P(C=c \mid M=m) = P(C=c)$$

$$P(C=c) = \underbrace{\sum P(C=c \mid M=m)}_{\text{const}} \cdot P(M=m)$$

$$P(C=c \mid M=m') = P(C=c \mid M=m)$$

$P(M=m) = 0.5$

$P(M=m') = 0.1$

$$P(M=m \mid C=c) = P(M=m)$$
$$P(M=m' \mid C=c) = P(M=m')$$

$\neq$ QED refuted.

4. a) $f(n) < \frac{1}{pol_1(n)}$ $\qquad g(n) < \frac{1}{pol_2(n)}$

$$f(n) \cdot g(n) < \frac{1}{pol_1(n) \cdot pol_2(n)}$$

QED

b) $f(n) = \frac{1}{2^n}$ $\qquad g(n) = \frac{1}{4^n}$ $\leftarrow$ counter example

$$f(n)/g(n) = \frac{2^{2n}}{2^n} = 2^n \nless \frac{1}{pol(n)}$$

QED

5. $$P[A(f(n)) = y \mid f(n) = f(y)] \leq negl$$
$$P[A(g(n)) = y \mid g(n) = g(y)] \leq negl$$

a) $P(A(f(x) \oplus g(x)) = y \mid f(x) \oplus g(x) = f(y) \oplus g(y)) \leq ngl(|x|)$ $\leftarrow$ wrong.

for any given $a, b, c$ & $d$ st $a \oplus b = c \oplus d$. and $|a| = |b| = |c| = |d| = |x|$

$P(a \oplus b = c \oplus d) \propto \left(\frac{6}{16}\right)^{|x|}$.

a). Counter example: $f = g$.

then $f \oplus g = 0$ for all inputs $x \Rightarrow$ not one way function

b) $h(x) = f(g(x))$

assume $A$ for $h(x)$.

$f(x)$ is OWF

$|f(x)| = |x|$ $\Big\}$ $f(x)$ is a bijection of the same space on itself

[$f$, $x$ have same space]

$\Rightarrow$ $A$ for $h(x)$ is also for $f(x)$

[contradiction]

c)

This $f'$ **is** one-way. In fact, this holds even if only $f$ is one-way (regardless of $g$, as long as $g$ is efficiently-computable). To see this, fix a PPT adversary $\mathcal{A}'$ and let

$$\epsilon(n) \stackrel{\text{def}}{=} \Pr[\mathcal{A}'(f'(x)) \text{ outputs an inverse of } f'(x)],$$

where the probability is taken over uniform choice of $x$ and the random coins of $\mathcal{A}'$. Consider the following PPT adversary $\mathcal{A}$: given input $y_1$ (which is equal to $f(x_1)$ for randomly-chosen $x_1$), choose random $x_2$, compute $y_2 := g(x_2)$, and run $\mathcal{A}'(y_1\|y_2)$. Then output the first half of the string output by $\mathcal{A}'$. It is not hard to see that (1) the input $y_1\|y_2$ given to $\mathcal{A}'$ is distributed identically to $f'(x_1\|x_2)$ for randomly-chosen $x_1, x_2$. This implies that $\mathcal{A}'$ inverts its input with probability $\epsilon(n)$. Furthermore, (2) whenever $\mathcal{A}'$ successfully inverts its input, $\mathcal{A}$ successfully inverts its own input. We conclude that $\mathcal{A}$ outputs an inverse of $y_1$ with probability at least $\epsilon(n)$, showing that $\epsilon$ must be negligible.

d) $h(x_1, x_2) = (f(x_1), x_2)$

$A$, $P[A(h(x_1,x_2)) = y_1, y_2 \mid h(y_1,y_2) = h(x_1,x_2)] \not\leq$ negl.

$y_2 = x_2$

$\boxed{f(y_1) = f(x_1)}$ not poss by PPTM $A$

$\therefore$ contradiction.

6. $G$ is a function, st Length of output = $\ell$(length of input) ??

a) $s$ is an n-bit binary string (random)

$y_0 = G(s)$ $\qquad y_1 \xleftarrow{R} \{0,1\}^{\ell(n)}$

b) $b$ is a random bit ($b \in \{0,1\}$)

c) give $y_b$ to $A$. $A$ outputs $b'$ (Ideal: if $y_0$, output 0. if $y_1$, output 1)

$\hookrightarrow$ constructing $A$: $A(y_b) = D_1(y_b) \begin{cases} 0 & \text{if } y_b = y_0 \\ 1 & \text{if } y_b = y_1 \end{cases}$

For any adversary $A$ interacting with the given experiment, we have that

$$\begin{aligned}
\Pr[b' = b] &= \Pr[b' = 0 \mid b = 0] \cdot \Pr[b = 0] + \Pr[b' = 1 \mid b = 1] \cdot \Pr[b = 1] \\
&= \frac{1}{2} \cdot \Pr[A(G(s)) = 0] + \frac{1}{2} \cdot \Pr[A(r) = 1] \\
&= \frac{1}{2} \cdot \Big(1 - \Pr[A(G(s)) = 1]\Big) + \frac{1}{2} \cdot \Pr[A(r) = 1] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \Big(\Pr[A(r) = 1] - \Pr[A(G(s)) = 1]\Big).
\end{aligned}$$

So $\left|\Pr[b' = b] - \frac{1}{2}\right| \leq \mathsf{negl}(n)$ iff $\Big|\Pr[A(r) = 1] - \Pr[A(G(s)) = 1]\Big| \leq \mathsf{negl}(n)$.

$P(b' = b) \leq \frac{1}{2} + \epsilon(n)$

$P(A(y_b) = b) \leq \frac{1}{2} + \epsilon(n)$.

$P(A(y_0) = 0) + P(A(y_1) = 1) \leq 1 + \epsilon(n)$

And $P(A(y_0) = 0) = 1 - P(A(y_0) = 1)$

Since $G$ is PRG,

$P(A(y_0) = 0) \leq \frac{1}{2} + \epsilon(n)$

$P(A(y_1) = 1) \leq \frac{1}{2} + \epsilon(n)$ $\Big\}$ $\frac{1}{2} + \epsilon(n) \leq \frac{1}{2}[1 - P(A(y_0) = 1) + P(A(y_1) = 1)]$

$\leq \frac{1}{2} + \frac{1}{2}[P(A(y_1) = 1) - P(A(y_0) = 1)]$

$\Rightarrow P[A(y_1) = 1] - P[A(y_0) = 1] \leq$ negl.

$\Downarrow$ leap

$P(D(y_0) = 1) \leq \frac{1}{2} + \epsilon(n)$

$P(D(y_1) = 1) \leq \frac{1}{2} + \epsilon(n)$

7. 1 year: $1.21 \times 10^{34}$ J

flip 1 bit: $5.8 \times 10^{-23}$ J.

flip 256 bits: $2^{256} \times 5.8 \times 10^{-23}$ J

time in years: $\dfrac{2^{256} \times 5.8 \times 10^{-23} \text{ J}}{1.21 \times 10^{34} \text{ J}} = 2^{256} \times 4.79 \times 10^{-57}$ years

$$\boxed{\begin{array}{l} 2^{10} > 10^{3} \\ 2^{190} > 10^{57} \\ 2^{190} \simeq 1.6 \times 10^{57} \end{array}}$$

$2^{256} \times 3 \times 2^{-190}$

$3 \times 2^{66}$

Not Possible

8. Let $G$ be a function that maps strings of length $n$ to strings of length $2n$. Define

$$\gamma(n) \stackrel{\text{def}}{=} \Pr[\text{the } (n+1)^{th} \text{ bit of } G(x) \text{ is equal to } 1]$$

where the probability is taken over random choice of $x \in \{0,1\}^n$. Prove that if $G$ is a pseudorandom generator, then there is a negligible function $\epsilon$ with $\gamma(n) \leq 1/2 + \epsilon(n)$. (Give a formal proof, not just an intuitive argument.)

8. G is a PRG.

in a purely random 2n-bit string, distribution of 0,1 bits is 1:1

in G, if $\gamma(n) \geq \frac{1}{2}$ + negl, then $\gamma(n)$ can act as a distinguisher for G (differing distribution compared to random)

contradicts the assumption that G is a PRG.

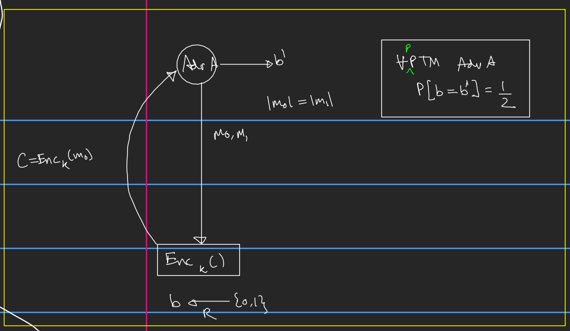
$\therefore$ $\gamma(n) \leq \frac{1}{2}$ + negl.

2n

n+1 1.

0, 1

9.




**Equivalent Definition of Perfect Secrecy**

An encryption scheme is $\boxed{\text{ciphertext-only secure}}$ if
$\forall$ PTM $A$, $P[b=b'] \le \frac{1}{2} + negl(n)$
(P of selecting correct message from the message space is negligibly more than random)

9. a) $m_1 = c_1 \oplus G(k)$

$m_2 = c_2 \oplus c_1$

b) eq. def: $P[b=b'] \le \frac{1}{2} + negl.$

but, $m_0 = m_a m_b$ $m_1 = m_c m_d$ $b = m_0$ or $m_1$

we get $c' = c_x c_y$

we can get $m_y$ from $c_x \oplus c_y$

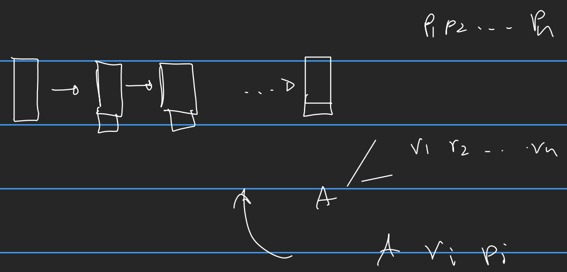
↳ $m_y = m_b$ or $m_d$ ⇒ we know the message

⇒ $P[b=b'] = 1$ violation QED.

10. a) OWP → PRG.

$G^{n+1}$ = OWP || h(OWP)

$G^{n+1} \to G^*$




Contra

b) $2^{l(n)} \to 2^n$

c) Consider a function $F_k$ taking 1 bit input and n bit output.

$F_k(0) = G_0(k)$ $F_k(1) = G_1(k)$

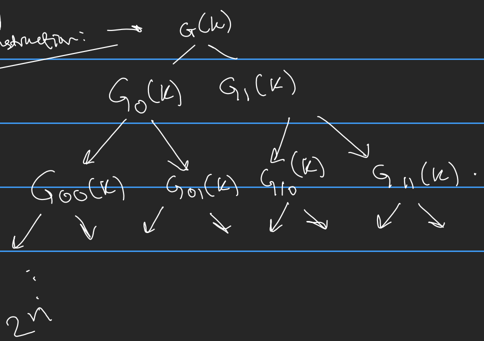
these are PRFs.

Now, for n-bit input → $F_k(r) = G_{r_{n-1}}(\dots G_{r_2}(G_{r_1}(G_{r_0}(k)))\dots)$

← constructed PRF

where, $r = r_0 r_1 r_2 \dots r_{n-1}$, $r_i \in \{0,1\}$

Construction: →




$k \in \{0,1\}^n$

**Proof of PRFness**

If there is a distinguisher which distinguishes $G_{01}(k)$ from truly random, then it can distinguish $G_0(k)$ which is not possible as $G_0(k)$ is a pseudo random generator.

Or

ii) PRGs ⇒ PRFs

$G : \{0,1\}^n \longrightarrow \{0,1\}^{2n}$

Let $G_0(s)$ = Left half of $G(s)$

$G_1(s)$ = right half of $G(s)$

Here $G(s) = G_0(s) \,||\, G_1(s)$

$k \in \{0,1\}^n$ , $r \in \{0,1\}^n$

$F_k(r) = G_{r_{n-1}}\left[G_{r_{n-2}}\left[\cdots G_{r_2}\left[G_{r_1}\left[G_{r_0}(k)\right]\right]\cdots\right]\right]$

TP: $\forall$ PPTM $\left|P\left(D^{F_k(\cdot)}(1^n)=1\right) - P\left(D^{R(\cdot)}(1^n)=1\right)\right| \leq negl(n)$

Assume to the contrary that $\exists$ a PPTM D.

Base Case: For $|r| = 1$, $F_k(r) = G_{r_0}(k)$

clearly if D can distinguish $F_k(r)$ then it can distinguish G.

Inductive Hypo: We cannot distinguish upto r of length n.

Consider r of length n+1.

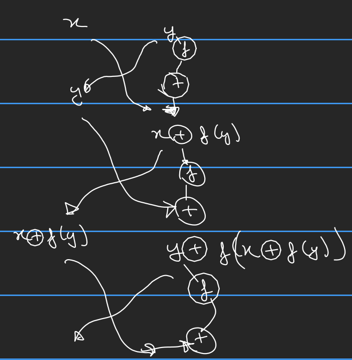
If we can distinguish $F_k(r)$

d). how to make PRF invertible without breaching pseudorandom property

use "Feistel structure".

if you have $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ (PRF)

if we have 2 inputs, $(x, y)$



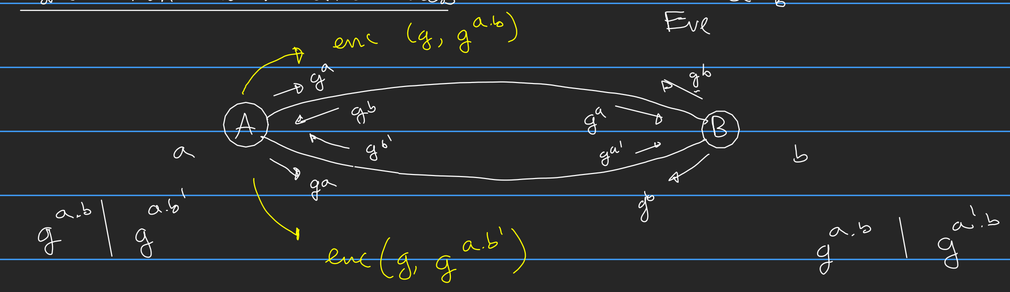

Data Encryption standard (DES)

without provable PRF, cannot say.

But 16 rounds of Feistel might do.

4 rounds of Feistel Structure, with proven a non-invertible PRF, then we get a bijected PRF(PRP) = block cipher

## Diffie-Helman with write access



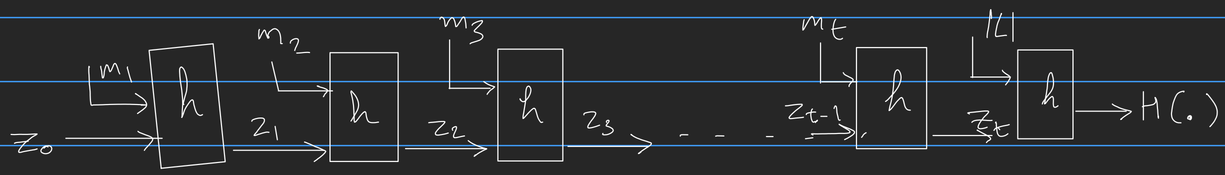

$g^{a.b}$ ✓ $g^{ab.}$

$g^{a.b}$ ✗ $g^{a'.b}$

$g^{ab'}$ ✗ $g^{ab}$

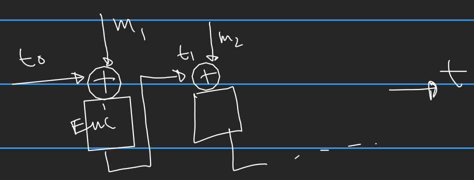
$g^{ab'}$ ✗ $g^{a'b}$

2. $|m_i| = n \qquad |z_i| = 2n$




3. $(m, t)$

$(m', t')$




$\underbrace{m'[0] \oplus t \;\; || \; m}_{\text{attack.}}$