EE817/IS 893

Cryptography Engineering and Cryptocurrency

Yongdae Kim

한국과학기술원

Z_n, Z_n^*

- The integers modulo n denoted by $\mathbf{Z_n}$ is the set of integers 0,1,2…n-1.
  - Z_{12} ={0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
- **$a \equiv b \pmod{n}$ if $n \mid a - b$**
- Let $a \in Z_n$, the **multiplicative inverse** of a is an integer $x \in Z_n$, s.t. $ax \equiv 1 \pmod{n}$
  - $5x \equiv 1 \pmod{12} \rightarrow x \equiv 5 \pmod{12}$
  - $5x \equiv 1 \pmod{14} \rightarrow x \equiv 11 \pmod{14}$
- **a is invertible iff gcd(a,n) = 1**
- **$Z_n^* = \{ a \in Z_n \mid \gcd(a,n)=1 \}$**
  - Z_{12}^* ={1, 5, 7, 11}, Z_{14}^* ={1, 3, 5, 9, 11, 13}
  - If n is a prime then $Z_n^* = \{ a \in Z_n \mid 1 \le a \le n-1 \}$

CRT

- Given r integers which are *pairwise relatively prime*, m_1, $m_2, \cdots, m_r$, then

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$x \equiv b_3 \pmod{m_3}$$
$$\cdots.$$
$$x \equiv b_r \pmod{m_r}$$

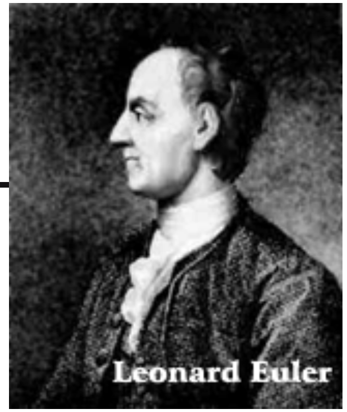
has the unique solution :

$$x = y_1 b_1 M_1 + \cdots + y_r b_r M_r \mod M$$

where $M = \prod m_i$, $M_i = M/m_i$, $y_i M_i \equiv 1 \pmod{m_i}$.

- Proof: check if x is a solution.

Fermat and Euler



- Fermat's little Theorem
  - Let p be a prime
  - if $\gcd(a,p)=1$ then $a^{p-1} \equiv 1 \pmod p$
- Euler's theorem: If $a \in Z_n^*$, then $a^{\Phi(n)} = 1 \pmod n$
  - Recap
    - $\phi(n)$: number of relatively prime integers to n in $\{0, 1, 2, \cdots, n-1\}$
    - $\phi(p) = p-1$, $\phi(p^r) = p^{r-1}(p-1)$, $\phi(pq) = (p-1)(q-1)$
  - Proof
    - Let $Z_n^* = \{r_1, r_2, \cdots, r_{f(n)}\}$.
    - Since $(a, n) = 1$ and $(r_i, n) = 1$, $(a\, r_i, n) = 1$.
    - Then $\{ar_1, ar_2, \cdots, ar_{f(n)}\}$ is a permutation of Z_n^*.
    - $r_1 r_2 \cdots r_{f(n)} = ar_1\, ar_2 \cdots ar_{f(n)} \bmod n$
- corollary: if n is a product of distinct primes and if $r \equiv s \bmod \Phi(n)$, then $a^r \equiv a^s \pmod n$

Fermat and Euler (Examples)

- $Z_7^* = \{1, 2, 3, 4, 5, 6\}$
  - $2^6 \bmod 7 \equiv 64 \bmod 7 \equiv 1$
  - $2^2 \bmod 7 \equiv 4$
  - $2^8 \bmod 7 \equiv 256 \bmod 7 \equiv 4$
- $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
  - $\phi(21) = \phi(3)\ \phi(7) = 2 * 6 = 12$
  - $2^{12} \bmod 21 \equiv 2048 \bmod 21 \equiv ((195 * 21)+1) \bmod 21 \equiv 1$
- if n is a product of two primes then

  $a^{k\phi(n)+1} \equiv a \pmod n$ for all integers a
  - $a^{k\phi(n)+1} \equiv (a^{\phi(n)})^k a^1 \equiv a$
- RSA: $n = p\ q$, $ed \equiv 1 \bmod \phi(n)$
  - Encryption: $c \equiv m^e \bmod n$
  - Decryption: $m' \equiv c^d \bmod n \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m$

Application of Euler's Theorem

- $2^{3216783}$ mod 17, 17: prime

  $\equiv 2^{3216783 \bmod 16} \bmod 17$

  $\equiv 2^{11} \bmod 17$

  $\equiv 8$

- $2^{2^{289}}$ mod 647, 647 = 17*19*2+1, prime

  $\equiv 2^{2^{289} \bmod 646} \bmod 647$

  $\equiv 2^{2^{289 \bmod 288} \bmod 646} \bmod 647$

  $\equiv 4 \bmod 647$

Generator

- Let $a \in Z_n^*$. The order of a ($ord_n(a)$) is the least positive t s.t. $a^t \equiv 1 \pmod{n}$

- if $t = \Phi(n)$ then a is said to be a **generator** of Z_n^*

- $ord_n(a)$ must divide $\Phi(n)$
  - Dual) $ord_p a \mid p - 1$

- If $a^v = 1 \bmod n$, then $ord_n a \mid v$.

Generator (cnt.)

- a is a generator iff $a^{\phi(n)/p} \neq 1 \bmod n$ for each prime divisor p of $\phi(n)$

  Proof)

  $\Rightarrow$) obvious, since a is a generator.

  $\Leftarrow$) Proof by contrapositive

  - Suppose a is not a generator $\Rightarrow$ Let $ord_n(a) = k < f(n)$. Then, $k \mid \phi(n)$.
  - Since k is a proper-divisor of $\phi(n)$, k has to divide $\phi(n)/p$ for some $p \mid \phi(n)$. $\Rightarrow$ $k\,q = \phi(n)/p$.
  - $a^{\phi(n)/p} = (a^k)^q = 1^q = 1 \bmod n$.

Generator (examples)

- Example: $Z_7^* = \{1,2,3,4,5,6\}$, $\phi(7) = 6 = 2 * 3$
  - $ord_7(1) = 1$ because $1^1 = 1$
    - is not generator since $1^2 \bmod 7 \equiv 1$
  - $ord_7(2) = 3$ because $2^3 = 1$
    - is not generator since $2^2 \bmod 7 \not\equiv 1$, but $2^3 \bmod 7 \equiv 1$
  - $ord_7(3) = 6$ because $3^6 = 1$ (3, 2, 6, 4, 5, 1)
    - is a generator since $3^2 \bmod 7 \not\equiv 1$, but $3^3 \bmod 7 \not\equiv 1$
  - $ord_7(4) = 3$ because $4^3 = 1$
    - is not generator since $4^2 \bmod 7 \not\equiv 1$, but $4^3 \bmod 7 \equiv 1$
  - $ord_7(5) = 6$ because $5^6 = 1$
    - is a generator since $5^2 \bmod 7 \not\equiv 1$, but $5^3 \bmod 7 \not\equiv 1$
  - $ord_7(6) = 2$ because $6^2 = 1$
    - is not generator since $6^2 \bmod 7 \equiv 1$, but $6^3 \bmod 7 \not\equiv 1$

Generator (example)

- Find all generators of Z_{17}^*.
  - What do you need to check?
    - $\phi(17) = 16 = 2^4$
    - Therefore, 2 is the only prime divisor of $\phi(17)$
    - So it is sufficient to check $a^8 \equiv ?\ 1 \bmod 17$.
  - $2^8 \bmod 17 \equiv 1$ (Not generator)
    - Then we don't need to check 1, 4, 8, 16. Why?
    - Furthermore, 15, 13, 9. Why?
  - $3^8 \bmod 17 \equiv 16$ (Good!)
  - $5^8 \bmod 17 \equiv 16$ (Good!)
  - $7^8 \bmod 17 \equiv 16$ (Good!)
  - $11^8 \bmod 17 \equiv 16$ (Good!)
  - 3, 5, 7, 11, 6, 10, 12, 14 are generators. Hmm… Any relation?

- Let $a \in Z_m^*$ and $ord(a) = h$. Then $ord(a^k) = h/gcd(h, k)$.

Square-and-Multiply

- $2^{13} \bmod 17 = 2^{2^\wedge 3+2^\wedge 2+1} \bmod 17 = (((2^2)^2)^2)\ ((2^2)^2)\ 2$
- INPUT: $a \in Z_n$, and $k < n$ where $k = S^t_{i=0} k_i 2^i$
- OUTPUT: $a^k \bmod n$.
- Algorithm
  - Set $b = 1$. If $k = 0$ then return(b).
  - Set $A = a$.
  - If $k_0 = 1$ then set $b = a$.
  - For i from 1 to t do the following:
    - Set $A = A^2 \bmod n$.
    - If $k_i = 1$ then set $b = A\ b \bmod n$.
  - Return(b).

Square-and-Multiply

- $a = 2$
- $k = 13$
- $n = 17$
- $k = S^{t}_{i=0} k_i 2^i$

- Set $A = a$.
- If $k_0 = 1$ then set $b = a$.
- For i from 1 to t
  - Set $A = A^2 \bmod n$.
  - If $k_i = 1$, set $b = Ab \bmod n$.

i	k_i	b	A
			2
0	1	2	2
1	0		2^2
2	1		$(2^2)^2$
		$2\ (2^2)^2$	$(2^2)^2$
3	1		$((2^2)^2)^2$
		$2\ (2^2)^2\ ((2^2)^2)^2$	

Factorization and DLP

- Used extensively in cryptography to build one-way function

- Integer factorization problem
  - Given a positive integer n, find its prime factorization

- Discrete Logarithm problem
  - Discrete Logarithm
    - The discrete logarithm of y to the base g mod p is x such that $y = g^x \bmod p$.
  - DLP: Given p, a generator g of Z_p^*, and an element $y \in Z_p^*$, find the integer x such that $g^x = y \bmod p$.

Integer Factorization Problem

- Trial division
  - If we try to find a factor by trial division, what is the complexity of the algorithm?
  - Initial thought: until n
  - Little improved: until n/2

- Eratosthenes Sieve
  - Sufficient to test up to sqrt(n)

RSA Encryption



- **Key Generation**
  - two large random primes p and q, each roughly the same size
  - $n = pq$, $f(n) = (p-1)(q-1)$
  - e, $1 < e < f(n)$, such that $\gcd(f(n), e) = 1$
  - $ed \equiv 1 \bmod f(n)$
  - A's public key is (n, e); A's private key is d
- **Encryption**: compute $c = m^e \bmod n$
- **Decryption**: $m = c^d \bmod n$
- Why?
  - $c^d \bmod n = m^{ed} \bmod n = m^{1 \bmod f(n)} \bmod n$

    $= m^{1 + k f(n)} \bmod n = m$

if n is a product of distinct primes and if $r=s \bmod f(n)$, then $a^r=a^s \pmod n$ for all a in Z_n^*

Security of RSA

- Factoring vs. RSA
  - Factor $\Longrightarrow$ RSAP
    - Trivial!!!
  - computing d from (n, e) and factoring n are computationally equivalent
    - $ed \equiv 1 \pmod{f(n)} \Longrightarrow \exists\, k$ such that $ed - 1 = k\, f(n)$
    - $a^{ed-1} \equiv 1 \pmod{n}$ for all $a \in Z_n^*$
    - Let $ed - 1 = 2^s t$, where t : odd
    - Then $\exists\, i \in [1, s]$ such that $a^{2^{i-1}t} \mathrel{!\equiv} \pm 1 \pmod{n}$, $a^{2^i t} \equiv 1 \pmod{n}$ for at least half of all $a \in Z_n^*$ (**)
    - if a and i are such integers then $\gcd(a^{2^{i-1}t} - 1,\ n)$ is a non-trivial factor of n
  - (**) $a^2 = 1 \bmod n$ has four solutions: 1, -1, a, -a

More explanation

- (**) $a^2 = 1 \bmod n$ has four solutions: 1, -1, a, -a
  - $a^2 = 1 \bmod p$ has two solutions 1, -1 mod p
  - $a^2 = 1 \bmod q$ has two solutions 1, -1 mod q

  - $a = 1 \bmod p$ and $a = 1 \bmod q$ ➔ $a = 1 \bmod pq$
  - $a = -1 \bmod p$ and $a = -1 \bmod q$ ➔ $a = -1 \bmod pq$
  - $a = 1 \bmod p$ and $a = -1 \bmod q$ ➔ $a = b \bmod pq$
  - $a = -1 \bmod p$ and $a = 1 \bmod q$ ➔ $a = -b \bmod pq$
- Example: $n = 7 \times 11$
  - $a^2 = 1 \bmod 7$ has two solutions 1, 6 mod 7
  - $a^2 = 1 \bmod 11$ has two solutions 1, 10 mod 11
  - $a = 1 \bmod 7$ and $a = 1 \bmod 11$ ➔ $a = 1 \bmod 77$
  - $a = -1 \bmod 7$ and $a = -1 \bmod 11$ ➔ $a = 76 \bmod 77$
  - $a = 1 \bmod 7$ and $a = -1 \bmod 11$ ➔ $a = b \bmod 77$ ➔ use CRT
    - where $M = 77$, $M_1 = M/m_1 = 11$, $M_2 = M/m_2 = 7$
    - $y_1M_1 = 1 \pmod{m_1}$ ➔ $y_1 11 = 1 \pmod{7}$ ➔ $y_1 = 2$
    - $y_2M_2 = 1 \pmod{m_2}$ ➔ $y_2 7 = 1 \pmod{11}$ ➔ $y_2 = 8$
    - $x = y_1 b_1M_1 + y_2b_2M_2 \bmod M = 2\ 1\ 11 + 8\ (-1)\ 7 = -34 = 43 \bmod 77$
  - $a = -1 \bmod 7$ and $a = 1 \bmod 11$ ➔ $a = -b \bmod 77 = 34 \bmod 77$

Security of RSA

- n cannot be shared
  - From the previous fact, (e, d, n) can be used to factor n.

- Small encryption exponent $e = 3$
  - When A wants to send message m to three entities whose $e = 3$, distinct n.
  - $c_i = m^3 \bmod n_i$, $i = 1, 2, 3$
  - Since n_i's are relatively prime, we can find x such that $x = c_1 \bmod n_1 = c_2 \bmod n_2 = c_3 \bmod n_3$.
  - Since $m^3 < n_1 n_2 n_3$, $x = m^3$.
  - Now, integer operation! Easy…
  - Padding required

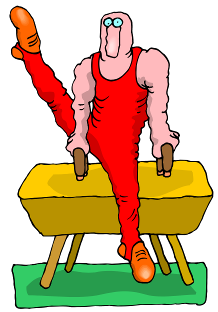
Security of RSA (cntd.)

- Forward Search Attack
  - If message space is small, eve can make dictionary (make c for all possible m)

- Homomorphic (multiplicative) property
  - $c_1 = m_1^e \bmod n, \; c_2 = m_2^e \bmod n$
  - $c_1 c_2 = (m_1^e \bmod n)(m_2^e \bmod n) = (m_1 m_2)^e \bmod n$
  - Without knowing plaintext, we can find ciphertext!
  - Which forgery?

RSA Encryption in Practice

- Recommended size of modulus > 1024



- Selecting primes
  - Roughly same size p and q to prevent elliptic curve factoring
  - $p - q$ should be large enough (attacking numbers near $sqrt(n)$)
  - Strong prime
    - $p - 1$ has large prime factor $r \Leftarrow$ Pollard $p - 1$ factoring
    - $p + 1$ has large prime factor $\Leftarrow$ $p + 1$ factoring algorithm
    - $r - 1$ has large prime factor $\Leftarrow$ cycling attacks
    - Random p, q has good property in general
- Selecting e
  - In general 3 or $2^{16}+1 = 65537$

Group

- A nonempty set G and operator $\circ$, $(G, \circ)$ is a **group** if:
  - **CLOSURE**: for all $x, y \in G$, $x \circ y \in G$
  - **ASSOCIATIVITY**: $\forall\, x, y, z \in G$, $(x \circ y) \circ z = x \circ (y \circ z)$
  - **IDENTITY**: $\exists\, 1 \in G$ such that $\forall\, x \in G$, $1 \circ x = x = x \circ 1$
  - **INVERSE**: $\forall\, x \in G$, $\exists$ inverse element $x^{-1} \in G$ such that $x^{-1} \circ x = 1 = x \circ x^{-1}$

- A group $(G, \circ)$ is **ABELIAN** if:
  - **COMMUTATIVITY**: for all $x, y \in G$, $x \circ y = y \circ x$
- A group G is *finite* if $|G|$ is finite. The number of elements in a finite group is called its *order*.

Examples

- $Z = \{\cdots -2, -1, 0, 1, 2, \cdots\}$ under + is a group
  - We call it $(Z, +)$
  - Abelian?

- $(Z, \bullet)$ group?

- $Z_n = \{0, 1, 2, \cdots, n-1\}$ group?

- M = Set of all 2 X 2 matrix
  - $(M, +)$ Abelian group?
  - $(M, \bullet)$ group?

Cyclic Groups

- An element $g \in G$ is a **group generator** of group $(G, \circ)$ if for all $x \in G$, \$ i such that

  $x = g^i = g \circ g \circ g \circ \cdots \circ g$ (i times), $G = \langle g \rangle$
- Definition: $(G, \circ)$ is **cyclic** if $\exists$ group generator.
- Definition: Group **order** of a group $(G, \circ)$ is **the size of set G**, i.e., $|G|$ or $\#\{G\}$ or $ord(G)$
- Definition: Group $(G, \circ)$ is **finite** if $ord(G)$ is fixed.
- Example: the set Z_n with addition modulo n is a group. Z_n with multiplication modulo n is not a group. Z_n^* is a group of order $f(n)$

Cyclic Groups

- An element $g \in G$ is a **group generator** of group $(G, \circ)$ if for all $x \in G$, $ i such that

  $x = g^i = g \circ g \circ g \circ \cdots \circ g$ (i times), $G = \langle g \rangle$
- Definition: $(G, \circ)$ is **cyclic** if $\exists$ group generator.
- Definition: Group **order** of a group $(G, \circ)$ is **the size of set G**, i.e., $|G|$ or $\#\{G\}$ or $\mathrm{ord}(G)$
- Definition: Group $(G, \circ)$ is **finite** if $\mathrm{ord}(G)$ is fixed.
- Example
  - $(Z_n, +\ \mathrm{mod}\ n)$ is a cyclic group. generator?
  - $(Z_p^*, \bullet\ \mathrm{mod}\ n)$ is a cyclic group. generator?

Examples

- $Q = \{a/b \mid a,b \in Z,\ b \neq 0\}$
  - $(Q, +)$: group
    - the rationals are closed under addition
    - the identity is 0
    - the inverse of x is -x
    - the rationals are associative
    - the rationals are commutative (so the group is abelian)
  - $(Q-\{0\}, *)$: group
    - the rationals are closed under multiplication
    - the identity is 1
    - the inverse of x is 1/x
    - the rationals are associative
    - the rationals are commutative (so the group is abelian)

Examples (cnt.)

- Z_p
  - $(Z_p, +)$
    - integers mod p are closed under +
    - the identity is 0
    - the inverse of x: -x \equiv p-x mod p
    - + is associative
    - + is commutative (so the group is abelian)
  - $(Z_p^*, \bullet)$
    - integers mod p are closed under $\bullet$
    - the identity is 1
    - the inverse of x: $x^{-1} = x^{p-2}$ mod p
    - $\bullet$ is associative
    - $\bullet$ is commutative (so the group is abelian)

Subgroup

- $(H, \circ)$ is a **subgroup** of $(G, \circ)$ if:
  - H is a subset of G
  - $a \circ b \in H$ for all $a,b \in H$
  - $ identity
  - $ $a^{-1} \in H$ for all $a \in H$.
- Example: $G = Z_7^* = \{1,2,3,4,5,6\}$, $H = \{1,2,4\}$
  - H is closed under multiplication mod 7
  - 1 is still the identity
  - 1 is 1 inverse, 2 and 4 are inverses of each other
- Lagrange Theorem (slight variation)
  - Let G be a multiplicative group of order n. For any g in G, ord(g) divides n.

Discrete Logarithm Problem

- Discrete Logarithm problem
  - Discrete Logarithm
    - The discrete logarithm of y to the base g modulus p is x such that $y = g^x \bmod p$
  - DLP: Given p, a generator g of Z_p^*, and an element $y \in Z_p^*$, find the integer x such that $g^x = y \bmod p$.
  - GDLP: Given a generator g of cyclic group G, and an element $y \in G$, find the integer x such that $g^x = y$.
- Best Algorithms
  - Pollard's rho: O(sqrt(q)) where q is the group size.
  - Index calculus: $L_p[1/3, c]$

Diffie-Hellman

- New Directions in cryptography
  - Whitfield Diffie, Martin E. Hellman, IEEE Transactions on Information Theory, 1976
- Setting
- $Z_p^* = \{1, 2, \cdots, p-1\}$, g -generator
- Protocol
  - $A \rightarrow B : N_A = g^{n1} \bmod p$
  - $B \rightarrow A : N_B = g^{n2} \bmod p$
  - $A : N_B^{n1} = g^{n1n2} \bmod p$
  - $B : N_A^{n2} = g^{n1n2} \bmod p$
- Diffie-Hellman Key : $g^{n1\,n2}$

Diffie-Hellman

- To set up a key shared between two parties who never met before
- Security
  - DLP → Diffie-Hellman problem?
  - Diffie-Hellman problem → DLP?
  - Authentication?

DLP in subgroup of Z_p^*

- Efficient and Secure construction
  - $Z_p^* = \{1, 2, \cdots, p-1\}$, g' - generator
  - $p = k\,q + 1$ ($|p| = 1024$, $|q| = 160$)
  - $g = g'^{k}$, $ord_p(g) = q$
  - $G = \langle g \rangle$
- When $p = k\,q + 1$ with $|p|=1024$, $|q| = 160$ (e.g.)
  - With Pollard's rho: O(sqrt(q))
  - With Index calculus: Lp[1/3, c]
  - So best in min of above two
- That's why we choose the above parameter and also Hash function

Better Implementation of DH

Setting

- $Z_p^* = \{1, 2, \cdots, p-1\}$, g' - generator
- $p = kq + 1$ ($|p| = 1024$, $|q| = 160$)
- $g = g'^k$, $ord_p(g) = q$

Protocol

- $A \rightarrow B : N_A = g^{n1} \bmod p$
- $B \rightarrow A : N_B = g^{n2} \bmod p$
- $A : N_B^{\ n1} = g^{n1n2} \bmod p$, $B : N_A^{\ n2} = g^{n1n2} \bmod p$

Security

- With Pollard's rho: O(sqrt(q))
- With Index calculus: Lp[1/3, c]

More Discussion on DH

- Long-term vs. Short-term DH
  - Short-term DH
    - When n_1 and n_2 are fresh, you can always generate a session (symmetric) key between two entities with two messages.
  - Long-term DH
    - When A has (nA, g^{nA}) and B has (nB, g^{nB}) as (private, public) key pair, A and B can compute their long-term symmetric key without any message.
    - Does not provide forward/backward security: when either one's private key is compromised, their pair-wise key is compromised.
- Authentication is required!
- Note that you can build DH on any group.
  - Elliptic curve DH is a DH protocol on top of a group on elliptic curve.

ElGamal Public Key Encryption

Key Generation

- prime p and a generator g of Z_p^*
- A's public key is $y=g^x$, A's private key is x

Encryption

- generate random integer k and compute $r = g^k \bmod p$
- compute $c = m\, y^k \bmod p$
- ciphertext (r, c)

Decryption

- $m = c\, r^{-a} \bmod p$

Discussions on ElGamal

- Efficiency
  - 2 mod exp, 2 times message expansion

- Security
  - Randomized encryption
    - precluding or decreasing CCA
  - Use fresh k for each encryption
    - $c_1 / c_2 = m_1 / m_2$ if k is same

SysSec
System Security Lab

Comparison: RSA vs. ElGamal

- Speed
  - Encryption Speed
    - RSA
    - ElGamal
  - Decryption Speed
    - RSA
    - ElGamal
- Message Expansion
  - RSA
  - ElGamal
- Public Key Size
- When do you want to use what?

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"