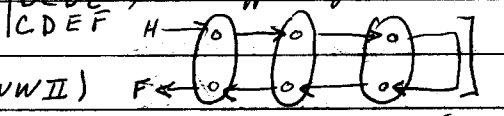
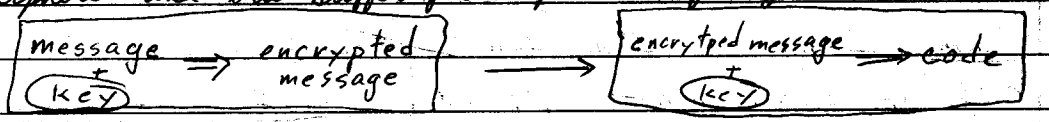
Cryptography

12/19/05

- caesar shift cipher: a b c d / D E F G, so ab ↦ DG
- even substitution ciphers are prone to easy decryption.
  - they are vulnerable to frequency analysis
- ex: Vigenere square | A B C D / B C D E / C D E F |, use different for each letter: we ↦ xg, etc.



- enigma machine (WWII)
  - total of $26^3 \simeq 70{,}000$ alphabets $\times \binom{26}{2}\binom{24}{2}\binom{20}{2}$, etc.
  - Germans had this technology, but ultimately lost due to improper use of the machine by the military users
- ciphers like this suffer from problem of key distribution



- two solutions: 1) Diffie-Hellman key exchange
  2) RSA encryption
- exponentiation mod n
- lemma: a polynomial $f(x) \in F[x]$ of degree n has at most n roots.
  - pf: If $f(a) = 0$ then consider $f(x) = (x-a)g(x) + r$, $r \in F$. evaluate at $a \Rightarrow r = 0$. Induct. □
- ~~proof~~:
- let F be a finite field. $\exists\ \mathbb{Z} \longrightarrow F$ (not injective). Kernel is $n\mathbb{Z} \Rightarrow \mathbb{Z}/n\mathbb{Z} \simeq$ image in $F \Rightarrow n = p$ a prime $\Rightarrow F$ is a finite dim. vector space over $\mathbb{Z}/p\mathbb{Z} \Rightarrow \#F = p^r = q$.
- prop: If $\#F = p^r$, then $F^\times = F - \{0\}$ is cyclic of order $p^r - 1$.
  - pf: for any $a \in F^\times$, $a^{q-1} = 1$. So all of $F^\times$ is a root of $x^{q-1} - 1 = 0$. So elements of $F^\times$ are $(q-1)$-st roots of unity. $F^\times \simeq \mathbb{Z}/d_1 + \cdots + \mathbb{Z}/d_k$, $d_1 | \cdots | d_k$. $\Rightarrow$ all of $F^\times$ is a root of $x^{d_k} - 1 = 0 \Rightarrow d_k = q-1$, $F^\times \simeq \mathbb{Z}/q-1$, by struct. thm. abel. grps. Thus, $F = \{$roots of $x^2 - x = 0\}$.
- Alice / Bob

Together pick a large prime $p \sim 2^{500}$ and generator g for $(\mathbb{Z}/p\mathbb{Z})^\times$

Alice picks some a mod p Bob picks some b mod p

Alice	Bob	Aside: $2^{11} \bmod 9$
$A = g^a$, sends $\longrightarrow$	$B = g^b$, sends $= 2^{1011_B} \bmod 9$	
	$\longleftarrow$	so compute $\log_2 n$ squares mod m
Key $= g^{ab} = A^b = B^a$ for both		Eve intercepts A, B, p, and g. Needs to solve $g^a = A \bmod p$ for $a \Rightarrow$ very hard, known as Discrete Log Problem

- This is the Diffie-Hellman solution, although not the most famous - RSA
- lemma: $(m,n) = 1 \Rightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $am + bn = 1$
  - pf: use the Euclidean algorithm.
- Claim: $\mathbb{Z}/mn \xrightarrow{\sim} \mathbb{Z}/m \times \mathbb{Z}/n$ if $(m,n) = 1$
  - pf: $am + bn = 1$, $am \mapsto (0,1)$ and $bn \mapsto (1,0)$, so surjectivity, and orders are same. □

  recall: $\mathbb{Z} \supset^{m} \mathbb{Z} \supset^{n} mn\mathbb{Z}$, so $m\mathbb{Z}/mn\mathbb{Z} \subset \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$
- In particular, $(\mathbb{Z}/mn)^\times \simeq (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$

Aside: $ak + bn = 1$, $g^{ak} = g$. Claim: k^{th} root of g is g^a. Example: find $\sqrt[5]{2} \pmod{13}$. $5 \cdot 5 - 2 \cdot 12 = 1$, so 2^5 is 5^{th} root of 2, $2^5 \equiv 6 \pmod{13}$

- Say G is a finite abelian gp. of order n, and $k < n$ s.t. $\gcd(k,n) = 1$. Then for every $g \in G$ $\exists!\, h \in G$ s.t. $h^k = g$.
  - pf: consider the homomorphism $\varphi: G \to G$ s.t. $h \mapsto h^k$. Claim $\ker \varphi = \{e\}$. Say $h \in \ker \varphi$. Then $h^k = e = h^n$, $\exists\, a, b \in \mathbb{Z}$ s.t. $ak + bn = 1 \Rightarrow h = h^{ak+bn} = e$. By ctg, hom. is surjective $\Rightarrow \forall g \in G\ \exists!\, h^k = g$.
- RSA Encryption (public key encryption)
- Take two large primes p, q, $n = pq$. $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. This has order $\varphi(n) = (p-1)(q-1)$ ← "Euler φ function"
- Pick k relatively prime to $\varphi(n)$. Publish (n, k).
- To send message to me: $a \bmod n$, compute $b = a^k \bmod n$, send me b.
  - this is secure, because we don't know p, q, so we don't know the order of the groups
  - finding d s.t. $b^d = a$, need k and $\varphi(n)$, and finding $\varphi(n)$ is equivalent to factoring n, as $\varphi(n) = n - p - q + 1$, so $p+q$ roots of $x^2 - \varphi(n)x + n$.