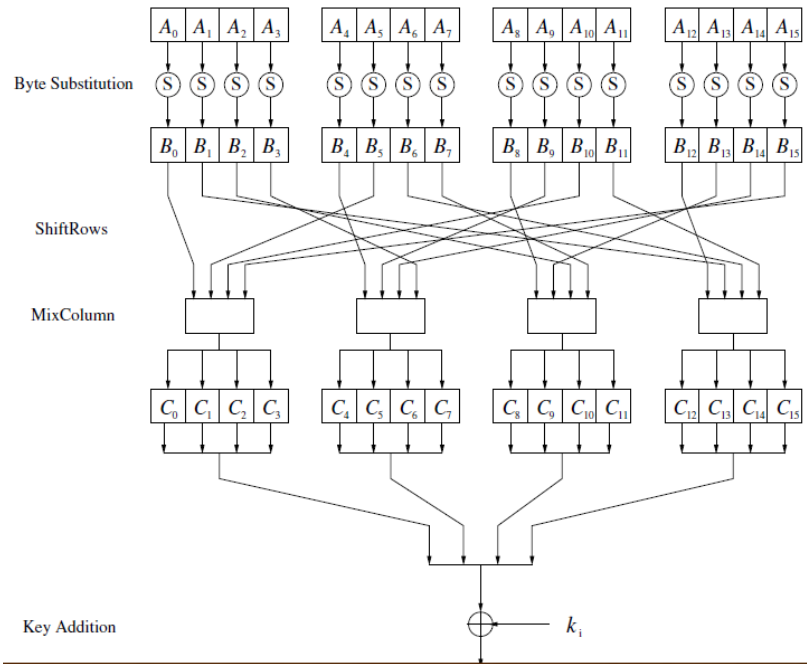
Cryptography – summary

- Proof of H(X; Y) = H(X) + H(Y |X) = H(Y) + H(X|Y) (chainrule).

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X},y\in\mathcal{Y}} p(x,y)\log\left(\frac{p(x)}{p(x,y)}\right) \\ &= -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} p(x,y)\log(p(x,y)) + \sum_{x\in\mathcal{X},y\in\mathcal{Y}} p(x,y)\log(p(x)) \\ &= H(X,Y) + \sum_{x\in\mathcal{X}} p(x)\log(p(x)) \\ &= H(X,Y) - H(X). \end{aligned}$$

  上面第一行没有错，就是除法上下反了一下，因此前面没有了负号

- DES: After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes
  就是为了让加密解密的图都一致，最后一轮加密了右半部分，然后交换为左半部分，然后执行下一轮操作就成了解密最后一轮。
- DES: S transform 48bit →32bit.就是 8*6 个 bit，从 8 个 S-box 自己对应的那一个中挑，每个 s-box 包含 2^6 也就是 64 个 entries，6bit 里面，第一和最后的 bit 来挑行，剩下 4bit 挑列，都是看成一个 2 进制数来算。
- S-Box 就是上面的 s transform: the only nonlinear element in the algorithm and provide confusion.
- AES: a single round



- The subbytes is the only non-linear in AES, it is bijective(所以可以用 look up table), but it does not have any fixed points
- 在 AES 的 key generation 中，通过产生单个 word 时，rotates its four input bytes, perform s-box substitution, add a round coefficient RC to the 1st byte, it add nonlinearity to the key and removes symmetry in AES as well.
- AES: subbytes 里面是先找加洛瓦域中的 inverse, 之后用 affine，后面这个 affine transformation 是固定的，就用这个矩阵和这个数。

- 加洛瓦域： $A^{-1}(x) \cdot A(x) = 1 \bmod P(x)$

  二进制都可以写成如下多项式的样子

  $$(x^7 + x^6 + x) \cdot (x^5 + x^3 + x^2 + x + 1) \equiv 1 \mod P(x).$$

  For AES, the irreducible polynomial:

  $$P(x) = x^8 + x^4 + x^3 + x + 1$$

- a ≡ r mod m, m is called the modulus and r is called the remainder
- 9 equivalence classes for modulus 9, e.g.
  {. . . ,−26,−17,−8, 1, 10,19,28, . . .}
  So, remainders are not unique.
  We always choose those in 0 ~ n-1
- Integer ring:
  The integer ring Zm consists of:
  1. The set Zm = {0,1,2, . . . ,m−1}
  2. Two operations "+" and "×" for all a,b ∈ Zm such that:
  a+b ≡ c mod m , (c ∈ Zm)
  a×b ≡ d mod m , (d ∈ Zm)
  其实就是很常见的环，和为余 0，就是负的，乘积为余 1 就是倒数
- Properties of above ring:
  1. Communitive and distributive laws hold
  2. Additive inverse exists for every element
  3. Multiplicative inverse exists only for some of element: if exists inverse, then b/a ≡ b · a^{-1} mod m.
  4. So we can add, subtract, multiply and [some time] divide.
- An element a ∈ Zm has a multiplicative inverse a^{-1} if and only if gcd(a,m) = 1
- gcd(0,n) = n
- 计算 Z*m 中的个数，也就是 phi-function

  Theorem 6.3.1 *Let m have the following canonical factorization*

  $$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n},$$

  where the p_i *are distinct prime numbers and* e_i *are positive integers, then*

  $$\Phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1}).$$

- If a 的多少次方 mod n 余 1，那么 a 就有 mod n 上面的逆，那么 a,n 互质
- 13*13 mod 17 = -4*-4 mod 17 = 16
- 找 a mod b 的 multiplicative inverse，就用 extended Euclidean algorithm 算 gcd(a,b)
- Extended Euclidean algorithm: 就是把需要的保留一个(比如 0，1 或者 gcd)，剩下的回代
- Math:
- Group: a group is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element and that satisfies four

conditions called the group axioms, namely closure, associativity, identity and invertibility.

- Group is commutative i.e. abelian.
- A Group is set with one operation and the corresponding inverse operation. If the operation is called addition, the inverse operation is subtraction; if the operation is multiplication, the inverse operation is division
- Field 就是两个 group mix 加一个分配律
- finite fields i.e. Galois fields. The number of elements in the field is called the order or cardinality of the field.
- A field with order m only exists if m is a prime power, i.e., $m = p^n$, for some positive integer n and prime integer p. p is called the characteristic of the finite field
- Zp = {0,1,2,...,p-1}
- Galois field with elements number not a prime，如 2^8 就不是 prime，则得重新定义加和乘法操作，简单来说就是当作 polynomial，然后每一个 x 指数单独 mod 2(因为在 $F[2^m]$上，其实看成异或也可以),之后的结果再除以 P
- Multiplicative inverse for 0 does not exists, AES s-box map 0 to 0.
- $P(x) = x^8+x^4+x^3+x+1$
  可以替换成 $x^8 \equiv x^4+x^3+x+1 \bmod P(x)$，这种方式来替代高次，然后 mod 好算
- A square matrix is singular(not invertible) if and only if its determinant is 0
- Determinant:

$$|A| = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}$$
$$= aei + bfg + cdh - ceg - bdi - afh.$$

- Matrix inverse:

	A_1	A_2	B_1	B_2
1	1	1/7	1/7	0
2	9	2	0	1

- Mod 26
  $5^{-1} = 21$
  $\begin{bmatrix} 2/5 & -1/5 \\ -9/5 & 7/5 \end{bmatrix}$ is equal to $\begin{bmatrix} 2 & -1 \\ -9 & 7 \end{bmatrix}$*21
- Mod 26 上矩阵 A 的逆,需要 det(A)的逆存在，也就是 gcd(n,det(A))=1
  A^{-1} =adjA/det A
  1. 每个 C 的小项是$(-1)^{i+j}$ · det(去掉第 i 行第 j 列)
  2. adjA 是 C^T
- index of coincidence:就是相同字母有多少对/所有可能的选择 C(n,2)
- conditional entropy:

$$H(X|Y) = -\sum_{j=1}^{d} P(Y=y_j) \sum_{i=1}^{m} P(X=x_i|Y=y_j) \log P(X=x_i|Y=y_j)$$
$$= -\sum_{i,j} P(X=x_i, Y=y_j) \log P(X=x_i|Y=y_j),$$

- 下面的证明 trick：
  把 log m 塞进去，或者把别的塞进去成为整体 ln，然后用 ln x≤x-1

Show $H(X \mid Y) - H(X) \leq 0$ which is equivalent to the claim.

$$\begin{aligned} H(X \mid Y) - H(X) &= -\sum_{i,j} p_{i,j} \log(p_{i|j}) + \sum_i p_i \log(p_i) \\ &= -\sum_{i,j} p_{i,j} \log\left(\frac{p_{i,j}}{p_j}\right) + \sum_i \underbrace{\sum_j p_{i,j}}_{=p_i} \log(p_i) \\ &= (\log e) \sum_{i,j:p_{i,j}>0} p_{i,j} \ln\left(\frac{p_i\, p_j}{p_{i,j}}\right) \\ &\overset{\ln(x)\leq x-1}{\leq} (\log e) \sum_{i,j:p_{i,j}>0} p_{i,j} \left(\frac{p_i\, p_j}{p_{i,j}} - 1\right) \\ &= (\log e) \sum_{i,j:p_{i,j}>0} (p_i\, p_j - p_{i,j}) = 0 \end{aligned}$$

- Conditional entropy chain rule:
  H(X1,X2,X3) = H(X3|X2,X1)+H(X2|X1)+H(X1)
- DES 明文和结果一样，并不能推出 k 一致。只能说很可能。
  https://crypto.stackexchange.com/questions/5492/brute-force-attack-on-des-property-of-des
- AES 对于 128 来说，有 10round，要 11key，k0 就是主 key 本来的样子
  0.K0 先 bytewise 异或
  1-9. 正常的四步 round，subbytes(加洛瓦域 inverse，然后 affine), shiftrows, mixcolumns(左边乘个矩阵), addroudnkey
  10.最后 1 round, 三步，subbytes, shiftrows, addroundkey
- primitive element 每个次方的余是所有 Z*n 的排列
  https://en.wikipedia.org/wiki/Primitive_root_modulo_n

Theorem 7.2. *Let $n \in \mathbb{N}$.*

a) There exists a primitive element modulo n if and only if

$$n \in \{2, 4, p^k, 2p^k \mid p \geq 3 \text{ prime}, k \in \mathbb{N}\}.$$

b) If there exists a primitive element modulo n, then there exist $\varphi(\varphi(n))$ many.

Proof. Exercise.

-

- P prime and p = 4k-1, then c 的平方根是$\pm c^k$ mod p
- **Proposition 9.2.** *(Euler's criterion) Let $p > 2$ be prime. $c \in \mathbb{Z}_p^*$ is a quadratic residue* mod p *if and only if* $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
- H(M|K,C)=0, H(C|M,K) =0
- H(K,C) =H(M,K,C); H(K,C) = H(M,K)
- If A,B stochastically independent, H(A,B) = H(A)+H(B) and H(A|B) = H(A)
- Perfect secrecy : H(M|C)=H(M) is equal to M,C stochastically independent
- If perfect secrecy, then |M+|≤|C+|≤|K+|
- DES: 64 bit block; 56 bit main key→48 bit key used
- SBB on Ri: expansion, xor with key, s-box, permutation, xor with Li
- Electronic Codebook Mode:直接用
  Cipher-Block Chaining Mode:明文和前一个密文异或后再加密
  Output Feedback Mode:单独 key stream，每个 key 是加密前一个 key，明文和 key 异或
  Cipher Feedback Mode:每个 key 是加密前一个密文，明文和 key 异或
  Counter Mode: key 自增 1，加密 key 后和明文异或